Version 9.6.0

December 2021

HITRUST CSF v9.6.0 Table of Contents

Change History

Version	Description of Change	Date Published
1.0	Final Version of Initial Release	September 2009
2.0	NIST SP 800-53 r2 PCI-DSS v1.2 HITECH ISO/IEC 27002 Rework	January 2010
2.1	State of Massachusetts 201 CMR 17.00 CMR 17.00	March 2010
2.2	Cloud Security Alliance Controls Matrix v1.0 Joint Commission (formerly JCAHO) Information Management State of Nevada NRS 603A	September 2010
3.0	CMS IS ARS v1-Appendix A (High)	December 2010
3.1	PCI-DSS v2.0	August 2011
4.0	NIST SP 800-53 r3 HIE WG Recommendations NIST-ISO-HIPAA Harmonization	December 2011
5.0	NIST SP 800-53 r4 (Feb 2012 IPD) Texas Health & Safety Code § 181 (TX HB 300) HITECH (MU Stage 2) CAQH Committee on Operating Rules for Information Exchange (CORE) NIST-CMS Harmonization Implementation Requirement Harmonization for HITRUST CSF 2013 Certification-required Controls	January 2013
6.0	NIST SP 800-53 r4 (Apr 2013 Final) CMS IS ARS v1.5 (2012) Title 1 TX Admin. Code 390.2 (TX Standards), including privacy requirements to support TX certification of the HIPAA Privacy Rule NIST-CMS Harmonization (publication updates)	February 2014
6.1	PCI-DSS v3.0 HIPAA Omnibus Rule NIST Cybersecurity Framework v1 ISO/IEC 27001:2013 ISO/IEC 27002:2013	April 2014
7.0	CMS IS ARS v2 (2013) HIPAA Omnibus Rule (updated Category 13 – Privacy Practices) NIST SP 800-53 r4 Appendix J MARS-E v1.0 IRS Pub 1075 (2014)	January 2015
8.0	AICPA Trust Services Criteria – Security, Availability, & Confidentiality HITRUST De-Identification Framework v1 PCI DSS v3.1 CSA CCM v3.0.1 CIS CSC v6 PMI DSP Principles & Framework v1 16 CFR 681 COBIT	February 2016
8.1	AICPA Trust Services Criteria (2016) PCI DSS v3.2 MARS-E v2	June 2016

Version	Description of Change	Date Published
9.0	DHS CRR EHNAC (additional requirements to support EHNAC Accreditation Assessments) Federal Register 21 CFR Part 11: Electronic Records; Electronic Signatures FedRAMP FFIEC IT Examination Handbook – Information Security, Sep 2016 OCR Audit Protocol Phase II (clarification of HIPAA Security requirements)	September 2017
9.1	European Union GDPR (General Data Protection Regulation) New York Department of Financial Services Title 23 NYCRR 500	February 2018
9.2	Category 13 restructure (language to reflect general privacy) APEC Privacy Framework EU GDPR control plain-language requirements HIPAA/Healthcare requirements moved to separate segment ISO/IEC 29100:2011 ISO/IEC 29151:2017 NIST SP 800-122 OECD Privacy Framework Singapore Personal Data Protection Act (PDPA)	January 2019
9.3	AICPA Trust Services Criteria (2017) – Security, Availability, Confidentiality, & Privacy California Consumer Privacy Act (CCPA) CIS CSC v7.1 CMS ARS v3.1 IRS Pub 1075 (2016) ISO/IEC 27799:2016 NIST Cybersecurity Framework v1.1 NIST SP 800-171 r2 PCI DSS v3.2.1 South Carolina Insurance Data Security Act (SCIDSA)	October 2019 *Includes updates as of November 2019*
9.4	CMMC v1.0 – including additional requirements to support CMMC Certification NIST SP 800-171 r2 (refreshed to ensure CMMC Alignment) Community Supplemental Requirements 002 NY DOH SSP v3.1	June 2020 *Includes updates as of July 2021*
9.5.0	HIPAA Security Rule (refresh) HIPAA Breach Notification (refresh)	September 2021
9.6.0	NIST SP 800-53 r4 (refresh)	December 2021

Control Category: 0.0 Information Security Management Program

Objective Name: 0.01 Information Security Management Program

Control Objective:	To implement and manage an Information Security Management Program.

Control Reference: 00.a Information Security Management Program

Control Specification:	An Information Security Management Program (ISMP) shall be defined in terms of the characteristics of the business, and established and managed including monitoring, maintenance, and improvement. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Audit and Accountability; Documentation and Records; IT Organization and Management Roles and Responsibilities; Monitoring; Planning; Policies and Procedures; Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to HIPAA Security Rule Subject to HITRUST De-ID Framework Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Privacy) Subject to Texas Health and Safety Code
Level 1 Implementation:	An Information Security Management Program (ISMP) is documented that addresses the overall Security Program of the organization. Management support for the ISMP is demonstrated through signed acceptance or approval by management. The ISMP considers all the HITRUST Control Objectives and documents any excluded control domains and the reasons for their exclusion. The ISMP is updated at least annually or when there are significant changes in the environment.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 45 CFR Part § 164.316(b)(1)(i) HIPAA.SR-1 45 CFR Part § 164.316(b)(2)(iii) HIPAA.SR-1 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 COBIT 5 APO13.02 COBIT 5 DS5.2 CRR v2016 CM:G1.Q1 CRR v2016 CM:G2.Q1 CRR v2016 CM:MIL2.Q1 CRR v2016 CM:MIL2.Q4 CRR v2016 SA:MIL2.Q2 CRR v2016 TA:MIL3.Q1 CRR v2016 VM:MIL3.Q1 CSA CCM v3.0.1 GRM-04 De-ID Framework v1 Privacy and Security Program: General FFIEC IS v2016 A.1.4

	FFIEC IS v2016 A.2.2 FFIEC IS v2016 A.2.3 ISO/IEC 27001:2013 4.4 NIST Cybersecurity Framework v1.1 ID.GV-1 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST SP 800-53 R4 AR-1[P]{0} NIST SP 800-53 R4 AT-1[HML]{0} NIST SP 800-53 R4 CA-1[HML]{0} NIST SP 800-53 R4 CM-1[HML]{0} NIST SP 800-53 R4 CP-1[HML]{0} NIST SP 800-53 R4 IA-1[HML]{0} NIST SP 800-53 R4 IR-1[HML]{0} NIST SP 800-53 R4 MA-1[HML]{0} NIST SP 800-53 R4 MP-1[HML]{0} NIST SP 800-53 R4 PE-1[HML]{0} NIST SP 800-53 R4 PL-1[HML]{0} NIST SP 800-53 R4 PM-1[HML]{0} NIST SP 800-53 R4 PS-1[HML]{0} NIST SP 800-53 R4 RA-1[HML]{0} NIST SP 800-53 R4 SA-1[HML]{0} NIST SP 800-53 R4 SC-1[H]{0} NIST SP 800-53 R4 SI-1[HML]{0} TJC IM.02.01.03, EP 1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to HIPAA Security Rule Subject to NY OHIP Moderate-Plus Security Baseline Subject to SCIDSA Requirements Subject to the EU GDPR
Level 2 Implementation:	Level 1 plus: The organization formally establishes, implements, operates, monitors, reviews, maintains, and improves the ISMP. The ISMP is formally documented, and such records are protected, controlled, and retained according to federal, state, and organizational requirements. The ISMP incorporates a Plan, Do, Check, Act (PDCA) cycle for continuous improvement in the ISMP, particularly as information is obtained that could improve the ISMP or indicates any shortcomings of the ISMP.
Level 2 Control Standard Mapping:	45 CFR Part § 164.316(a) HIPAA.SR-1 45 CFR Part § 164.316(b)(1)(i) HIPAA.SR-2 AICPA 2017 CC3.1 CMSRs v3.1 PM-01 (HIGH; MOD) COBIT 5 DS5.5 COBIT 5 DSS05.07 CRR v2016 CM:MIL2.Q2 FFIEC IS v2016 A.1.4 FFIEC IS v2016 A.2.2 FFIEC IS v2016 A.2.3

	FFIEC IS v2016 A.2.8 FFIEC IS v2016 A.6.1 ISO/IEC 27001:2013 10.1(c) ISO/IEC 27001:2013 10.2 ISO/IEC 27001:2013 4.4 ISO/IEC 27001:2013 5.1(a) ISO/IEC 27001:2013 5.2 ISO/IEC 27001:2013 5.3 ISO/IEC 27001:2013 6.1.1(c) ISO/IEC 27001:2013 6.1.1(d) ISO/IEC 27001:2013 6.1.1(e) ISO/IEC 27001:2013 6.2(e) ISO/IEC 27001:2013 7.1 ISO/IEC 27001:2013 7.4 ISO/IEC 27001:2013 7.5.1(a) ISO/IEC 27001:2013 7.5.2 ISO/IEC 27001:2013 7.5.3 ISO/IEC 27001:2013 8.1 ISO/IEC 27001:2013 8.2 ISO/IEC 27001:2013 8.3 ISO/IEC 27001:2013 9.1 ISO/IEC 27001:2013 9.2 ISO/IEC 27001:2013 9.3(b) ISO/IEC 27001:2013 9.3(f) MARS-E v2 PM-1 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 PR.IP-7 NY DOH SSP v3.1 PM-1a[M]-1 SCIDSA 33-99-20(G) TJC IM.02.01.03, EP 1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to 23 NYCRR 500 Subject to Banking Requirements Subject to CRR V2016 Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to State of Massachusetts Data Protection Act Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: Management provides evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the ISMP. The organization determines and provides the resources needed to establish, implement, operate, monitor, review, maintain and improve an ISMP. The organization ensures that all personnel who are assigned responsibilities defined in the ISMP are competent to perform the required tasks. The organization also ensures

	that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMP objectives. The organization conducts internal ISMP audits at planned intervals to determine the continuing suitability, adequacy, and effectiveness of the program. Management reviews the organization's ISMP at planned intervals (at least once a year) to ensure its continuing suitability, adequacy, and effectiveness. This review includes assessing opportunities for improvement and the need for changes to the ISMP, including the information security policy and information security objectives. The results of the reviews are clearly documented, and records maintained. The organization continually improves the effectiveness of the ISMP with the information security policy, information security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review.
Level 3 Control Standard Mapping:	AICPA 2017 CC4.1 CMSRs v3.1 PM-02 (HIGH; MOD) CMSRs v3.1 PM-03 (HIGH; MOD) CMSRs v3.1 PM-04 (HIGH; MOD) CMSRs v3.1 PM-06 (HIGH; MOD) CMSRs v3.1 PM-09 (HIGH; MOD) CMSRs v3.1 PM-13 (HIGH; MOD) COBIT 5 DS5.5 COBIT 5 DSS05.07 CRR v2016 CM:G4.Q1 FFIEC IS v2016 A.1.4 FFIEC IS v2016 A.2.3 FFIEC IS v2016 A.2.8 IRS Pub 1075 v2016 9.3.18.1 ISO/IEC 27001:2013 4.1 ISO/IEC 27001:2013 4.2(b) ISO/IEC 27001:2013 5.1(c) ISO/IEC 27001:2013 5.1(d) ISO/IEC 27001:2013 5.1(e) ISO/IEC 27001:2013 5.1(f) ISO/IEC 27001:2013 5.1(g) ISO/IEC 27001:2013 6.1.1 ISO/IEC 27001:2013 6.2 ISO/IEC 27001:2013 7.2 ISO/IEC 27001:2013 7.3(b) ISO/IEC 27001:2013 7.3(c) ISO/IEC 27001:2013 9.3 MARS-E v2 PM-13 MARS-E v2 PM-2 MARS-E v2 PM-3 MARS-E v2 PM-4 MARS-E v2 PM-6 MARS-E v2 PM-9 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 PR.AT-1 NIST Cybersecurity Framework v1.1 PR.AT-2 NIST Cybersecurity Framework v1.1 PR.AT-3 NIST Cybersecurity Framework v1.1 PR.AT-4 NIST Cybersecurity Framework v1.1 PR.AT-5 NIST Cybersecurity Framework v1.1 PR.IP-7

Level CMMC	Implementation Requirements
Level CMMC Implementation:	The organization establishes, maintains, and resources: an access control plan with a focus on: i) establishing system access requirements, ii) controlling internal system access, iii) controlling remote system access, and iv) limiting data access to authorized users and processes;

	an asset management plan with a focus on: i) identifying and documenting assets, ii) managing the asset inventory, iii) defining audit requirements, iv) performing audits, v) identifying and protecting audit information, and vi) reviewing and managing audit logs; an audit and accountability plan with a focus on: i) defining audit requirements, ii) performing audits, iii) identifying and protecting audit information, and iv) reviewing and managing audit logs; an awareness and training plan with a focus on: i) conducting security awareness activities, and ii) conducting training; a configuration management plan with a focus on: i) establishing configuration baselines, and ii) performing configuration and change management; an identification and authentication plan with a focus on granting access to authenticated entities; an incident response plan with a focus on: i) planning incident response, ii) detecting and reporting events, iii) developing and implementing a response to a declared incident, iv) performing post incident reviews, and v) testing incident response; a maintenance plan with a focus on managing maintenance; a media protection plan with a focus on: i) identifying and marking media, ii) protecting and controlling media, iii) sanitizing media, and iv) protecting media during transport; a personnel security plan with a focus on: i) screening personnel, and ii) protecting CUI during personnel actions; a physical protection plan with a focus on limiting physical access; a recovery plan with a focus on: i) managing backups, and ii) managing information security continuity; a risk management plan with a focus on: i) identifying and evaluating risk, ii) managing risk, and iii) managing supply chain risk; a security assessment plan with a focus on: i) developing and managing a system security plan, ii) defining and managing controls, and iii) performing code reviews; a situational awareness plan with a focus on implementing threat monitoring; a system and communications protection plan with a focus on: i) defining security requirements for systems and communications, and ii) controlling communications at system boundaries; and a system and information integrity plan with a focus on: i) identifying and managing information system flaws, ii) identifying malicious content, iii) performing network and system monitoring, and iv) implementing advanced email protections.

Level DGF Implementation Requirements

Level DGF Implementation:	The organization has a formally defined Data Governance program with defined vision and goals. A consistent framework is used to manage Data Governance. The Data Governance program and framework are reviewed when changes are required or at least annually.

Level EHNAC Implementation Requirements

Level EHNAC Implementation:	The organization must determine if they are a Hybrid organization as defined by HIPAA § 164.103 and, if so, describe which parts of the organization are subject to HIPAA regulations and demonstrate how they are isolated from other portions of the business.

Level FFIEC IS Implementation Requirements	
Level FFIEC IS Implementation:	Management implements metrics that demonstrate the extent to which the information security management program is implemented and whether the program is effective. The metrics implemented are timely, comprehensive, and actionable to improve the ISMPs effectiveness and efficiently.

Level HIX Implementation Requirements	
Level HIX Implementation:	The organization provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended. The organization has a formal information protection program based on an accepted industry framework that is reviewed and updated as needed, and the program plan is protected from unauthorized disclosure and modification.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation:	The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes ongoing security control assessments in accordance with the organizational continuous monitoring strategy. The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes reporting the security status of the organization and the information system to defined personnel or roles (defined in the applicable system security plan) monthly.

Level SCIDSA Implementation Requirements	
Level SCIDSA Implementation:	Licensees have a formal information security program that, based on a risk assessment, is designed to mitigate the identified risks, commensurate with the size, complexity, and the sensitivity of the data which the licensee holds. The licensee designates a specific person, affiliate, or entity to be responsible for the program. Annually, insurers are required to submit a written statement by the 15th of February, certifying compliance with the South Carolina Insurance Data Security Act and maintain all required records for a period of five years.

Level Title 23 NYCRR Part 500 Implementation Requirements	
Level Title 23 NYCRR Part 500 Implementation:	A covered entity required to comply with NYCRR 500 must implement a cybersecurity program that meets the requirements specified in NYCRR 500 or adopt a cybersecurity program maintained by an affiliated entity, provided the program satisfies the requirements specified in NYCRR 500.

	All documentation and information relevant to the covered entity's cybersecurity program must be made available to the Financial Services Superintendent of New York upon request. The covered entity must annually submit a written statement to the financial services superintendent of the state of New York certifying that the organization is compliant with the requirements set forth in document 23 NYCRR 500. The organization must maintain all records, schedules, and data supporting this certificate for a period of five years.

Control Category: 01.0 - Access Control

Objective Name: 01.01 Business Requirement for Access Control

Control Objective:	To control access to information, information assets, and business processes based on business and security requirements.

Control Reference: 01.a Access Control Policy

Control Specification:	An access control policy shall be established, documented, and reviewed based on business and security requirements for access.
Factor Type:	Organizational
Topics:	Audit and Accountability; Authentication; Authorization; Policies and Procedures; User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 1 Subject to CMMC Level 2 Subject to FISMA Compliance Subject to HIPAA Security Rule Subject to HITRUST De-ID Framework Requirements Subject to IRS Pub 1075 Compliance Subject to Joint Commission Accreditation Subject to MARS-E Requirements Subject to NIST 800-171 Basic Level Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Supplemental Requirements Subject to Texas Health and Safety Code Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	Access control rules account for and reflect the organization's policies for information dissemination and authorization, and these rules are supported by formal procedures and clearly defined responsibilities. Access control rules and rights for each user or group of users are clearly stated. Access controls are both logical and physical and these are considered together. Users and service providers are given a clear statement of the business requirements to be met by access controls. Specifically, the access control program take account of the following: 1. security requirements of individual business applications and business units (e.g., separation/segregation within a hybrid entity);

	2. information dissemination and authorization (e.g., need-to-know, need to share, and least privilege principles; security levels; and classification of information.) 3. relevant legislation and any contractual obligations regarding protection of access to data or services; 4. standard user access profiles for common job roles in the organization; 5. requirements for formal authorization of access requests; 6. requirements for emergency access; 7. requirements for periodic review of access controls; and 8. removal of access rights. The organization develops and disseminates/communicates a formal access control program (e.g., through policies and procedures) and reviews and updates the program annually.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 21 CFR Part 11.10(d) 45 CFR Part § 164.308(a)(3)(i) HIPAA.SR-0 45 CFR Part § 164.308(a)(4)(i) HIPAA.SR-0 45 CFR Part § 164.308(a)(4)(ii)(A) HIPAA.SR-0 45 CFR Part § 164.308(a)(4)(ii)(B) HIPAA.SR-0 45 CFR Part § 164.308(a)(4)(ii)(C) HIPAA.SR-0 45 CFR Part § 164.310(a)(2)(iii) HIPAA.SR-1 45 CFR Part § 164.312(a)(2)(ii) HIPAA.SR-0 AICPA 2017 CC5.2 AICPA 2017 CC6.1 AICPA 2017 CC6.2 AICPA 2017 CC6.3 AICPA 2017 CC6.4 AICPA 2017 CC6.8 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMMC v1.0 AC.1.001-0 CMMC v1.0 AC.2.007-0 CMMC v1.0 CM.2.062-0 CMSRs v3.1 AC-01 (HIGH; MOD) CMSRs v3.1 AC-02 (HIGH; MOD) CRR v2016 CCM:G2.Q10 CRR v2016 CCM:G2.Q4 CRR v2016 CCM:G2.Q8 CSA CCM v3.0.1 IAM-02 De-ID Framework v1 Access Control: General FedRAMP AC-1 FedRAMP AC-2 FFIEC IS v2016 A.6.22(d) FFIEC IS v2016 A.6.8(c) IRS Pub 1075 v2016 9.3.1.1 IRS Pub 1075 v2016 9.3.1.2 ISO/IEC 27002:2013 9.1.1 ISO/IEC 27799:2016 9.1.1 MARS-E v2 AC-1 MARS-E v2 AC-2 NIST 800-171 r2 3.1.1-0 NIST 800-171 r2 3.1.5-0 NIST 800-171 r2 3.4.6-0 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.AC-6 NIST SP 800-53 R4 AC-1[HML]{0} NIST SP 800-53 R4 AC-3(4)[S]{1} NIST SP 800-53 R4 AC-3(8)[S]{0} NIST SP 800-53 R4 AC-6[HM]{0} NIST SP 800-53 R4 SA-17(7)[S]{0} NY DOH SSP v3.1 AC-1a2[M]-0 NY DOH SSP v3.1 AC-1b[M]-0 NY DOH SSP v3.1 AC-1b1[M]-0 NY DOH SSP v3.1 AC-1b2[M]-0 NY DOH SSP v3.1 AC-2i1[M]-0 NY DOH SSP v3.1 AC-2i2[M]-2 NY DOH SSP v3.1 AC-6[M]-0

	NY DOH SSP v3.1 CM-5(5).IS1[M]-2 NY DOH SSP v3.1 CM-5(5)a[MN]-2 SR v6.4 16-0 SR v6.4 19-0 SR v6.4 41-1 SR v6.4 7b.1-2 TJC IM.02.01.03, EP 1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental)
Level 2 Implementation:	Level 1 plus: All information related to the business applications and the risks the information is facing is identified. The access control and information classification policies of different systems and networks are consistent. Access rights are managed in a distributed and networked environment ensuring all types of connections available are recognized. Access control roles (e.g., access request, access authorization, access administration) are segregated.
Level 2 Control Standard Mapping:	FFIEC IS v2016 A.6.8(c) ISO/IEC 27002:2013 9.1.1 ISO/IEC 27002:2013 9.1.2 ISO/IEC 27002:2013 9.2.1 ISO/IEC 27002:2013 9.2.2 ISO/IEC 27002:2013 9.2.3 ISO/IEC 27799:2016 9.1.1 ISO/IEC 27799:2016 9.1.2 ISO/IEC 27799:2016 9.2.1 NIST Cybersecurity Framework v1.1 ID.AM-5 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 AC-2i[HML]{1} NIST SP 800-53 R4 AC-3(2)[S]{1}

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The organization develops, documents, and disseminates to applicable personnel an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

	The organization only permits the use of shared/group accounts when a business need can be documented and approved, in advance, by the Authorizing Official (AO), and when used, the applicable System Security Plan (SSP) must: (i) describe how the shared/group accounts are used and (ii) include compensating processes and procedures implemented to provide the ability to uniquely attribute account user activities. Shared accounts must be restricted to specific devices and hours when possible. The information system enforces organization-defined circumstances and/or usage conditions for organization-defined information system accounts. If remote access is authorized, access to HHS Webmail using personally owned equipment is authorized. Access to other systems/networks using personally-owned equipment is prohibited without written authorization from the CIO, or an approved policy allowing the use of personally-owned equipment that specifies: (i) personally-owned equipment must be scanned before being connected to CMS (and HHS) systems or networks to ensure compliance with CMS requirements and (ii) personally-owned equipment must be prohibited from processing, accessing, or storing Department sensitive information unless it is approved in writing by the CMS SOP and employs CMS required encryption (FIPS 140-2 validated module). The organization restricts the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information. Prior to being provided access to PII on remote devices, device users must acknowledge through a binding agreement their responsibilities to safeguard the PII accessible from the device and that they are aware of and agree to the organization's capabilities to manage the organization's PII on the device, including confiscation, in consultation with the organization's counsel, if necessary to remove the PII. The organization employs defined automated mechanisms, or manual processes (defined in the applicable security plan), to assist users in making information sharing/collaboration decisions.

Objective Name: 01.02 Authorized Access to Information Systems

Control Objective:	To ensure authorized user accounts are registered, tracked, and periodically validated to prevent unauthorized access to information systems.

Control Reference: 01.b User Registration

Control Specification:	There shall be a formal documented and implemented user registration and de-registration procedure for granting and revoking access. *Required for HITRUST Certification CSF v9.6
Factor Type:	System
Topics:	Authorization; Monitoring; Policies and Procedures; User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1	Applicable to all systems

System Factors:	
Level 1 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 1 Subject to CMMC Level 3 Subject to HIPAA Security Rule Subject to IRS Pub 1075 Compliance Subject to Joint Commission Accreditation Subject to NIST 800-171 Basic Level Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to State of Massachusetts Data Protection Act Subject to Supplemental Requirements Subject to Texas Health and Safety Code
Level 1 Implementation:	The organization must maintain a current listing of all workforce members (individuals, contractors, vendors, business partners, etc.) with access to sensitive information (e.g., PII). User registration and de-registration formally addresses establishing, activating, modifying, reviewing, disabling, and removing accounts. At a minimum, the organization addresses how access requests to information systems are submitted, how access to the information systems is granted, how requests to access sensitive information are submitted, how access to sensitive information is granted, how authorization and/or supervisory approvals are verified, and how a workforce members level of access to sensitive information is verified. Account types are identified (individual, shared/group, system, application, guest/anonymous, emergency, and temporary) and conditions for group and role membership established. Access to the information systems is granted based on a valid need-to-know/need-to-share that is determined by assigned official duties and intended system usage. Such usage/access is granular enough to support an individual's consent that has been captured by the organization and limits access, use, or disclosure based on what is necessary to satisfy a particular purpose or carry out a function, or to provide separation/segregation between business units (e.g., within a hybrid entity). Access granted satisfies all personnel security criteria. Proper identification is required for requests to establish information system accounts and approval of all such requests. Guest/anonymous, shared/group, emergency and temporary accounts are specifically authorized, and use monitored. Unnecessary accounts are removed, disabled, or otherwise secured. Account managers are notified when users are terminated or transferred, their information system usage or need-to-know/need-to-share changes, or when accounts (including shared/group, emergency, and temporary accounts) are no longer required. Shared/group account credentials are modified when users are removed from the group. The access control procedure for user registration and de-registration: 1. communicates password procedures and policies to all users who have system access 2. checks that the user has authorization from the system owner for the use of the information system or service; 3. separates approval for access rights from management; 4. checks that the level of access granted is appropriate to the business purpose and is consistent with organizational security policy (e.g., it is consistent with sensitivity and risks associated with the information and/or information system, it does not compromise segregation of duties); 5. gives users a written statement of their access rights;

	6. requires users to sign statements indicating that they understand the conditions of access; 7. ensures service providers do not provide access until authorization procedures have been completed; 8. ensures default accounts are removed and/or renamed; 9. maintains a formal record of all persons registered to use the service; 10. removes or blocks critical access rights of users who have changed roles or jobs or left the organization immediately and removes or blocks non-critical access within 24 hours; and 11. automatically removes or disables accounts that have been inactive for a period of 60 days or more.
Level 1 Control Standard Mapping:	201 CMR 17.04(2)(a) 201 CMR 17.04(2)(b) 201 CMR 17.04(2)(d) 21 CFR Part 11.10(d) 21 CFR Part 11.10(g) 45 CFR Part § 164.308(a)(3)(ii)(B) HIPAA.SR-1 AICPA 2017 CC5.2 AICPA 2017 CC6.2 AICPA 2017 CC6.3 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CIS CSC v7.1 16.10 CIS CSC v7.1 16.7 CMMC v1.0 AC.1.002-0 CMMC v1.0 IA.3.086-0 CMSRs v3.1 AC-02 (HIGH; MOD) CMSRs v3.1 AC-02(03) (HIGH; MOD) CMSRs v3.1 IA-01 (HIGH; MOD) CMSRs v3.1 IA-04 (HIGH; MOD) CMSRs v3.1 IA-05 (HIGH; MOD) COBIT 5 DS5.3 CSA CCM v3.0.1 IAM-09 EHNAC Accreditation Committee FedRAMP AC-2 FedRAMP AC-2(10) FedRAMP AC-2(3) FedRAMP AC-2(4) FedRAMP AC-2(9) FedRAMP IA-1 FedRAMP IA-4 FedRAMP IA-5 FedRAMP PS-4 FFIEC IS v2016 A.6.20(a) FFIEC IS v2016 A.6.20(b) FFIEC IS v2016 A.6.20(e) FFIEC IS v2016 A.6.27(c) IRS Pub 1075 v2016 9.3.1.2 IRS Pub 1075 v2016 9.3.7.4 IRS Pub 1075 v2016 9.3.7.5 ISO/IEC 27001:2013 9.2.1 MARS-E v2 AC-2 MARS-E v2 AC-2(3) MARS-E v2 IA-1 MARS-E v2 IA-4 MARS-E v2 IA-5 NIST 800-171 r2 3.1.2-0 NIST 800-171 r2 3.5.6-0 NIST Cybersecurity Framework v1.1 DE.CM-3 NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.AC-6 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 AC-2(10)[S]{0} NIST SP 800-53 R4 AC-2c[HML]{0} NIST SP 800-53 R4 AC-2d[HML]{0} NIST SP 800-53 R4 AC-2e[HML]{0} NIST SP 800-53 R4 AC-2f[HML]{0} NIST SP 800-53 R4 AC-2h[HML]{0} NIST SP 800-53 R4 AC-2i[HML]{3} NIST SP 800-53 R4 AC-2k[HML]{0}

	NIST SP 800-53 R4 PS-3(3)a[S]{0} NIST SP 800-53 R4 PS-4f[HML]{0} NIST SP 800-53 R4 PS-5d[HML]{0} NIST SP 800-53 R4 PS-6(2)a[S]{0} NIST SP 800-53 R4 PS-6(2)b[S]{0} NY DOH SSP v3.1 AC-17.IS4d[M]-1 NY DOH SSP v3.1 AC-2(10)[MN]-0 NY DOH SSP v3.1 AC-2(9).NYS1[MN]-0 NY DOH SSP v3.1 AC-2.IS.PII2[M]-0 NY DOH SSP v3.1 AC-2.IS.PII6[M]-1 NY DOH SSP v3.1 AC-2.IS1[M]-1 NY DOH SSP v3.1 AC-2.IS1[M]-2 NY DOH SSP v3.1 AC-2.IS6[M]-0 NY DOH SSP v3.1 AC-2a[M]-0 NY DOH SSP v3.1 AC-2c[M]-0 NY DOH SSP v3.1 AC-2d[M]-3 NY DOH SSP v3.1 AC-2e[M]-0 NY DOH SSP v3.1 AC-2h1[M]-0 NY DOH SSP v3.1 AC-2h2[M]-0 NY DOH SSP v3.1 AC-2h3[M]-0 NY DOH SSP v3.1 AC-2i2[M]-3 NY DOH SSP v3.1 AC-2i3[M]-0 NY DOH SSP v3.1 AC-2k[M]-0 NY DOH SSP v3.1 PE-3a1[M]-0 NY DOH SSP v3.1 PS-3e2[M]-0 NY DOH SSP v3.1 PS-4(2).IS1[H]-2 NY DOH SSP v3.1 PS-4f[M]-2 NY DOH SSP v3.1 PS-5c[M]-0 OCR Audit Protocol (2016) 164.308(a)(3)(ii)(A) PCI DSS v3.2.1 8.1.2 PCI DSS v3.2.1 8.1.3 PCI DSS v3.2.1 8.1.4 PMI DSP Framework PR.AC-4 SR v6.4 19a-0 SR v6.4 19c-0 SR v6.4 6.5-0 TJC IM.02.01.03, EP 5

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Is the system(s) accessible from the Internet? Yes
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance
Level 2 Implementation:	Level 1 plus: The organization requires that the registration process to receive hardware administrative tokens and credentials used for two-factor authentication be verified in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor or other individual defined in an applicable security plan). Organizations do not use group, shared or generic accounts and passwords. Identity verification of the individual is required prior to establishing, assigning, or certifying an individual's electronic signature or any element of such signature.
Level 2 Control Standard Mapping:	201 CMR 17.04(1)(d) 21 CFR Part 11.10(d) 21 CFR Part 11.10(g)

	21 CFR Part 11.100(b) CMSRs v3.1 IA-05(03) (HIGH; MOD) COBIT 5 DS5.4 COBIT 5 DSS05.03 COBIT 5 DSS05.04 CSA CCM v3.0.1 IAM-08 FedRAMP IA-5 FedRAMP IA-5(3) ISO/IEC 27002:2013 9.2.1 ISO/IEC 27002:2013 9.2.2 ISO/IEC 27799:2016 9.2.1 ISO/IEC 27799:2016 9.2.2 MARS-E v2 IA-5(3) NIST Cybersecurity Framework v1.1 PR.AC-1 NIST SP 800-53 R4 IA-4(2)[S]{0} NIST SP 800-53 R4 IA-4(3)[S]{2} NIST SP 800-53 R4 IA-4(7)[S]{0} NIST SP 800-53 R4 IA-5(3)[HM]{0} NRS 603A.215.1 NY DOH SSP v3.1 AC-2.IS.PII1[M]-0 NY DOH SSP v3.1 IA-5(3)[M]-0 PCI DSS v3.2.1 8.5 TJC IM.02.01.03, EP 5

Level 3 Implementation Requirements

Level 3 Organizational Factors:	
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to FedRAMP Certification Subject to FISMA Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: The organization employs automated mechanisms to support the management of information system accounts. In addition to assigning a unique ID and password, at least one of the following methods is employed to authenticate all users: 1. token devices (e.g., SecurID, certificates, or public key); or 2. biometrics. The organization automatically disables emergency accounts within 24 hours and temporary accounts with a fixed duration not to exceed 30 days.
Level 3 Control Standard Mapping:	FedRAMP AC-2(1) MARS-E v2 AC-2(1) MARS-E v2 AC-2(2) NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST SP 800-53 R4 AC-2(1)[HM]{0} NIST SP 800-53 R4 AC-2(2)[HM]{0} NIST SP 800-53 R4 AC-2(8)[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 AC-2(1)[M]-0 PCI DSS v3.2.1 8.2 TJC IM.02.01.03, EP 5

Level CMS Implementation Requirements	
Level CMS Implementation:	The organization disables accounts of users posing a significant risk immediately, not to exceed 30 minutes after discovery of the risk. Automated mechanisms support the management of information system accounts, including the disabling of emergency accounts within 24 hours and temporary accounts within a fixed duration not to exceed 30 days.

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation:	Automated mechanisms support the management of information system accounts, including the disabling of emergency accounts within 24 hours and temporary accounts within a fixed duration not to exceed 30 days.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation:	The information system automatically disables inactive accounts within sixty [60] days. The information system automatically audits account creation, modification, enabling, disabling, and removal actions and notifies defined personnel or roles (defined in the applicable security plan). The organization disables accounts of users posing a significant risk within sixty [60] minutes of discovery of the risk.

Control Reference: 01.c Privilege Management

Control Specification:	The allocation and use of privileges to information systems and services shall be restricted and controlled. Special attention shall be given to the allocation of privileged access rights, which allow users to override system controls. *Required for HITRUST Certification CSF v9.6
Factor Type:	System
Topics:	Authorization; User Access

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to HIPAA Security Rule Subject to Joint Commission Accreditation Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to State of Massachusetts Data Protection Act Subject to Supplemental Requirements Subject to Texas Health and Safety Code

Level 1 Implementation:	The allocation of privileges for all systems and system components is controlled through a formal authorization process. The access privileges associated with each system product (e.g., operating system, database management system and each application) and the users to which they need to be allocated are identified. Privileges are allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy (i.e., the minimum requirement for their functional role, e.g., user or administrator, only when needed). At a minimum, the organization explicitly authorizes access to the following list of security functions (deployed in hardware, software, and firmware) and security-relevant information: 1. Setting/modifying audit logs and auditing behavior; 2. Setting/modifying boundary protection system rules; 3. Configuring/modifying access authorizations (i.e., permissions, privileges); 4. Setting/modifying authentication parameters; and 5. Setting/modifying system configurations and parameters. An authorization process and a record of all privileges allocated are maintained.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 201 CMR 17.04(2)(a) 21 CFR Part 11.10(d) 21 CFR Part 11.10(g) 45 CFR Part § 164.312(a)(1) HIPAA.SR-0 AICPA 2017 CC6.2 AICPA 2017 CC6.3 AICPA 2017 CC6.8 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 AC-06 (HIGH; MOD) CMSRs v3.1 AC-06(01) (HIGH; MOD) COBIT 5 DS5.4 COBIT 5 DSS05.04 CRR v2016 AM:G5.Q5 CRR v2016 CCM:G2.Q4 CRR v2016 CM:G2.Q10 CSA CCM v3.0.1 IAM-04 CSA CCM v3.0.1 IAM-09 De-ID Framework v1 Identification and Authentication (Application-level): Authentication Policy FedRAMP AC-6 FedRAMP AC-6(1) FFIEC IS v2016 A.6.20(d) FFIEC IS v2016 A.6.21(a) FFIEC IS v2016 A.6.22(b) FFIEC IS v2016 A.6.29 FFIEC IS v2016 A.6.8(c) IRS Pub 1075 v2016 9.3.1.6 ISO/IEC 27002:2013 9.2.3 ISO/IEC 27002:2013 9.2.3(b) ISO/IEC 27799:2016 9.2.3 MARS-E v2 AC-6 MARS-E v2 AC-6(1) NIST Cybersecurity Framework v1.1 PR.AC-4 NIST SP 800-53 R4 AC-21(2)[S]{0} NIST SP 800-53 R4 AC-3[HML]{0} NIST SP 800-53 R4 AC-6(1)[HM]{0} NIST SP 800-53 R4 AC-6(4)[S]{0} NY DOH SSP v3.1 AC-2d[M]-2 NY DOH SSP v3.1 AC-3.PII[M]-0 NY DOH SSP v3.1 AC-3[M]-0 NY DOH SSP v3.1 CM-7(2)c[M]-0 NY DOH SSP v3.1 PS-3(3)a[MN]-0 PCI DSS v3.2.1 7.1 PCI DSS v3.2.1 7.1.1 PCI DSS v3.2.1 7.1.4 PCI DSS v3.2.1 7.2.1 PCI DSS v3.2.1 7.2.2 SR v6.4 5-0

	SR v6.4 7a.1-0 SR v6.4 7a.3-0 SR v6.4 7b.1-1 TJC IM.02.01.03, EP 5

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Is the system(s) accessible from the Internet? Yes Number of interfaces to other systems 25 to 75 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CMMC Level 2 Subject to HITRUST De-ID Framework Requirements Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline
Level 2 Implementation:	Level 1 plus: Role-based access control is implemented and capable of mapping each user to one or more roles, and each role to one or more system functions. The development and use of system routines are promoted to avoid the need to grant privileges to users. The development and use of programs which avoid the need to run with elevated privileges are promoted. Elevated privileges are assigned to a different user ID from those used for normal business use. All users access privileged services in a single role (users registered with more than one role designate a single role during each system access session). The use of system administration privileges (any feature or facility of an information system that enables the user to override system or application controls) is minimized. Access to privileged functions (e.g., system-level software, administrator tools, scripts, utilities) deployed in hardware, software, and firmware is restricted. Security relevant information is restricted to explicitly authorized individuals. The organization facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to business partners match the access restrictions on information for specific circumstances in which user discretion is allowed. The organization also employs manual processes or automated mechanisms to assist users in making information sharing/collaboration decisions. The access control system for the system components storing, processing, or transmitting covered information is set with a default "deny-all" setting.
Level 2 Control Standard Mapping:	21 CFR Part 11.10(d) AICPA 2017 CC6.3 CMMC v1.0 AC.2.008-0 CMSRs v3.1 AC-02 (HIGH; MOD) CMSRs v3.1 AC-06 (HIGH; MOD) CMSRs v3.1 AC-06(01) (HIGH; MOD) CMSRs v3.1 AC-06(02) (HIGH; MOD) CMSRs v3.1 AC-10 (HIGH) CMSRs v3.1 AC-21 (HIGH; MOD) De-ID Framework v1 Access Control: Access Policies FedRAMP AC-2 FedRAMP AC-21 FedRAMP AC-6 FedRAMP AC-6(1) FedRAMP AC-6(2) FFIEC IS v2016 A.6.20(d) FFIEC IS v2016 A.6.22(b)

	FFIEC IS v2016 A.6.27(b) IRS Pub 1075 v2016 9.3.1.16 IRS Pub 1075 v2016 9.3.1.2 IRS Pub 1075 v2016 9.3.1.6 ISO/IEC 27002:2013 9.1.1 ISO/IEC 27002:2013 9.2.3 ISO/IEC 27799:2016 9.1.1 ISO/IEC 27799:2016 9.2.3 MARS-E v2 AC-10 MARS-E v2 AC-2 MARS-E v2 AC-6 MARS-E v2 AC-6(1) MARS-E v2 AC-6(2) NIST 800-171 r2 3.1.6-0 NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.AC-6 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.PT-4 NIST SP 800-53 R4 AC-21[HM]{0} NIST SP 800-53 R4 AC-6(5)[HM]{0} NY DOH SSP v3.1 AC-2.IS.PII4[M]-0 NY DOH SSP v3.1 AC-6(5)[M]-1 PCI DSS v3.2.1 7.1.2 PCI DSS v3.2.1 7.1.3 PCI DSS v3.2.1 7.2 PCI DSS v3.2.1 7.2.3 TJC IM.02.01.03, EP 5

Level 3 Implementation Requirements

Level 3 Organizational Factors:	
Level 3 System Factors:	Number of interfaces to other systems Greater than 75 Number of transactions per day Greater than 85,000 Number of users of the system(s) Greater than 5,500
Level 3 Regulatory Factors:	Subject to CMMC Level 3 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: The organization limits authorization to privileged accounts on information systems to a pre-defined subset of users and tracks and monitors privileged role assignments for anomalous behavior. The organization audits the execution of privileged functions on information systems and ensures information systems prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards (e.g., IDS/IPS or malicious code protection mechanisms). All file system access not explicitly required for system, application, and administrator functionality is disabled. Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems is restricted to personnel based upon the principle of least

	privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles). Contractors are provided with minimal system and physical access and agree to and support the organization's security requirements. The contractor selection process assesses the contractor's ability to adhere to and support the organization's security policy and procedures. The organization ensures only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of the users' job duties.
Level 3 Control Standard Mapping:	AICPA 2017 CC6.8 CIS CSC v7.1 14.6 CIS CSC v7.1 4.1 CMMC v1.0 AC.3.018-0 CMSRs v3.1 AC-06 (HIGH; MOD) CMSRs v3.1 AC-06(03) (HIGH) CMSRs v3.1 AC-06(03) (HIGH; MOD) CMSRs v3.1 AC-06(05) (HIGH; MOD) CMSRs v3.1 AC-06(09) (HIGH; MOD) CMSRs v3.1 AC-06(10) (HIGH; MOD) CMSRs v3.1 CM-07 (HIGH; MOD) CSA CCM v3.0.1 IVS-11 FedRAMP AC-6 FedRAMP AC-6(10) FedRAMP AC-6(5) FedRAMP AC-6(9) FedRAMP CM-7 IRS Pub 1075 v2016 9.3.1.6 IRS Pub 1075 v2016 9.3.10.6 IRS Pub 1075 v2016 9.3.5.7 IRS Pub 1075 v2016 9.4.11 IRS Pub 1075 v2016 9.4.9 IRS Pub 1075 v2016 Exhibit 10 ISO/IEC 27002:2013 9.2.3 ISO/IEC 27799:2016 9.2.3 MARS-E v2 AC-6 MARS-E v2 AC-6(10) MARS-E v2 AC-6(5) MARS-E v2 AC-6(9) MARS-E v2 CM-7 NIST 800-171 r2 3.1.7-0 NIST Cybersecurity Framework v1.1 DE.CM-3 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 ID.RM-1 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.PT-1 NIST SP 800-53 R4 AC-3(10)[S]{0} NIST SP 800-53 R4 AC-6(10)[HM]{0} NIST SP 800-53 R4 AC-6(6)[S]{0} NIST SP 800-53 R4 AC-6(8)[S]{0} NIST SP 800-53 R4 AC-6(9)[HM]{0} NIST SP 800-53 R4 CM-5(5)a[S]{1} NIST SP 800-53 R4 PS-7b[HML]{0} NRS 603A.215.1 NY DOH SSP v3.1 AC-2.IS3[M]-0 NY DOH SSP v3.1 AC-5.IS2[M]-2 NY DOH SSP v3.1 AC-6(10)[M]-0 NY DOH SSP v3.1 AC-6(9)[M]-0 NY DOH SSP v3.1 AC-6.IS1[M]-0 NY DOH SSP v3.1 AC-6.IS2[M]-0 NY DOH SSP v3.1 AC-6.IS4[M]-0 NY DOH SSP v3.1 CM-5(5).IS1[M]-1 NY DOH SSP v3.1 CM-5(5)a[MN]-1 NY DOH SSP v3.1 PS-7.IS1[HML]-0 TJC IM.02.01.03, EP 5

Level CIS Implementation Requirements

Level CIS Implementation:	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems is restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles). The organization uses automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges and validates that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive. Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not Internet browsing, email, or similar activities. Administrators use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine is isolated from the organization's primary network and not be allowed Internet access. This machine is not to be used for reading email, composing documents, or surfing the Internet. Contractors are provided with minimal system and physical access and agree to and support the organization's security requirements. The contractor selection process assesses the contractor's ability to adhere to and support the organization's security policy and procedures.

Level CMS Implementation Requirements

Level CMS Implementation:	All system and removable media boot access is disabled unless it is explicitly authorized by the organizational CIO for compelling operational needs. If system and removable media boot access is authorized, boot access is password protected. The organization authorizes network access to privileged commands only for compelling operational needs (defined in the applicable security plan) and documents the rationale for such access in the security plan for the information system.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	A role-based access approach is used to establish and administer privileged user accounts, including application-specific privileged user accounts based on the responsibilities associated with the use of each application, such roles are monitored, and actions are taken when privileged roles assignments are no longer appropriate.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	Business roles and rules are imbedded at either the authentication level or application level. In either case, the agency must ensure that only authorized employees or contractors (as allowed by statute) of the agency receiving the information have access to FTI. The agency must restrict the sharing/re-disclosure of FTI to only those authorized in IRC 6103 and as approved by the Office of Safeguards. The organization password-protects system initialization (boot) settings. The agency must restrict the use of information system media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, CDs, DVDs) on information

	systems that receive, process, store, or transmit FTI using physical or automated controls. Multifunction Device (MFD) access enforcement controls must be configured correctly, including access controls for file shares, administrator and non-administrator privileges, and document retention functions. To use FTI in a SAN environment, the agency must ensure: 1. access controls are implemented and strictly enforced for all SAN components to limit access to disks containing FTI to authorized users; and 2. fiber channel devices must be configured to authenticate other devices with which they communicate in the SAN and administrator connections. The least privilege principle must be strictly enforced in a virtualized environment. To use a virtual environment that receives, processes, stores, or transmits FTI, programs that control the hypervisor are secured and restricted to authorized administrators only.

Level HIE Implementation Requirements

Level HIE Implementation:	HIEs, for all employees and for all employees of connecting organizations, define and assign roles to each individual with access to the HIE. The roles are based on the individual's job function and responsibilities. The roles specify the type of access and level of access.

Level HIX Implementation Requirements

Level HIX Implementation:	A role-based access approach is used to establish and administer privileged user accounts, including application-specific privileged user accounts based on the responsibilities associated with the use of each application, and such roles are monitored. The information system does not release information outside of the established system boundary unless the receiving organization provides appropriate security safeguards, and the safeguards are used to validate the appropriateness of the information designated for release.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	Shared accounts must have strictly limited permissions and access only to the system(s) required. Restrict the use of database management utilities to only authorized database administrators. Prevent users from accessing database data files at the logical data view, field, or field-value level. Implement table-level access control. At a minimum, the organization explicitly authorizes access to the following list of security functions (deployed in hardware, software, and firmware) and security-relevant information: (i) setting/modifying audit logs and auditing behavior; (ii) setting/modifying boundary protection system rules; (iii) configuring/modifying access authorizations (i.e., permissions, privileges); (iv) setting/modifying authentication parameters; and (v) setting/modifying system configurations and parameters. At a minimum, the organization requires that users of information system accounts, or roles, with access to the following list of security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system

	functions, and if feasible, audits any use of privileged accounts, or roles, for such functions: (i) setting/modifying audit logs and auditing behavior; (ii) setting/modifying boundary protection system rules; (iii) configuring/modifying access authorizations (i.e., permissions, privileges); (iv) setting/modifying authentication parameters; and (v) setting/modifying system configurations and parameters. The information system limits the number of concurrent sessions for each system account to one [1] session for both normal and privileged users. The number of concurrent application/process sessions is limited and enforced to the number of sessions expressly required for the performance of job duties and any requirement for more than one [1] concurrent application/process session is documented in the security plan. The organization identifies employees and contractors who hold roles with significant information security and privacy responsibilities.

Level PCI Implementation Requirements

Level PCI Implementation:	A service provider protects each organization's hosted environment and data by: 1. ensuring that each organization only runs processes that only have access to that organization's cardholder data environment; and 2. restricting each organization's access and privileges to only its own cardholder data environment.

Control Reference: 01.d User Password Management

Control Specification:	Passwords shall be controlled through a formal management process. *Required for HITRUST Certification CSF v9.6
Factor Type:	System
Topics:	Authentication; Authorization; Cryptography; User Access; Password Management

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to CMMC Level 2 Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to State of Massachusetts Data Protection Act Subject to Supplemental Requirements
Level 1 Implementation:	The following controls are implemented to maintain the security of passwords: 1. passwords are prohibited from being displayed when entered; 2. passwords are changed whenever there is any indication of possible system or password compromise; and 3. user identity is verified before performing password resets.

	The allocation of passwords is controlled through a formal management process: 1. the use of third-parties or unprotected (clear text) electronic mail messages is avoided; 2. users acknowledge receipt of passwords; 3. default vendor passwords are altered following installation of systems or software; 4. temporary passwords are changed at the first log-on; 5. temporary passwords are given to users in a secure manner; 6. maintain a list of commonly-used, expected or compromised passwords, and update the list at least every 180 days and when organizational passwords are suspected to have been compromised directly or indirectly; 7. verify, when users create or update passwords, that the passwords are not found on the organization-defined list of commonly-used, expected, or compromised passwords; 8. transmit only cryptographically-protected passwords; 9. store passwords using an approved hash algorithm and salt, preferably using a keyed hash; 10. require immediate selection of a new password upon account recovery; 11. allow user-selection of long passwords and passphrases, including spaces and all printable characters; and 12. employ automated tools to assist the user in selecting strong passwords and authenticators. Alternatively, passwords/phrases must have a strength (entropy) at least equivalent to the parameters specified above. Password policies, applicable to mobile devices, are documented and enforced through technical controls on all company devices or devices approved for BYOD usage and prohibit the changing of password/PIN lengths and authentication requirements.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 201 CMR 17.04(1)(b) AICPA 2017 CC6.6 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 1 153: Eligibility and Benefits Connectivity Rule v1.1.0 Subsection 5.2 CIS CSC v7.1 16.5 CMMC v1.0 IA.2.080-0 CMMC v1.0 IA.2.081-0 CMSRs v3.1 IA-05 (HIGH; MOD) CMSRs v3.1 IA-05(01) (HIGH; MOD) CSA CCM v3.0.1 IAM-12 CSA CCM v3.0.1 MOS-16 FedRAMP IA-5 FedRAMP IA-5(4) FFIEC IS v2016 A.6.22(a) HITRUST IRS Pub 1075 v2016 9.3.1.16 IRS Pub 1075 v2016 9.3.7.5 ISO/IEC 27002:2013 9.2.4 ISO/IEC 27002:2013 9.3.1 ISO/IEC 27002:2013 9.4.2 ISO/IEC 27002:2013 9.4.3 ISO/IEC 27799:2016 9.2.4 ISO/IEC 27799:2016 9.3.1 ISO/IEC 27799:2016 9.4.2 ISO/IEC 27799:2016 9.4.3 MARS-E v2 IA-5 MARS-E v2 IA-5(1) NIST 800-171 r2 3.5.10-0 NIST 800-171 r2 3.5.9-0 NIST Cybersecurity Framework v1.1 PR.AC-1 NIST SP 800-53 R4 IA-5(4)[S]{0} NIST SP 800-53 R4 IA-6[HML]{0} NRS 603A.215.1 PCI DSS v3.2.1 2.1

	PCI DSS v3.2.1 8.2.2 PCI DSS v3.2.1 8.2.3 PCI DSS v3.2.1 8.2.4 PCI DSS v3.2.1 8.2.5 PCI DSS v3.2.1 8.2.6 SR v6.4 20.2-0 SR v6.4 22a-0 SR v6.4 22b-2 SR v6.4 22c-0 SR v6.4 23.2-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Is the system(s) accessible from the Internet? Yes Number of interfaces to other systems 25 to 75
Level 2 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The following controls are implemented to maintain the security of passwords: 1. passwords are protected from unauthorized disclosure and modification when stored and transmitted; 2. passwords are not included in any automated log-on process (e.g., stored in a macro or function key); 3. all passwords are encrypted during transmission and storage on all system components; 4. users sign a statement to keep personal passwords confidential and to keep group passwords solely within the members of the group; and 5. temporary passwords are unique to an individual and are not guessable. Persons who use electronic signatures based upon use of identification codes in combination with passwords employ controls to ensure their security and integrity. Such controls include: 1. maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password. 2. ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging); 3. following loss management procedures to electronically de-authorize lost, stolen, missing or otherwise potentially compromised tokens, cards and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls; 4. use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organization management; and 5. initial and periodic testing of devices, such as tokens or cards, which bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

	Electronic signatures that are not based upon biometrics: 1. Employ at least two distinct identification components (i.e., user ID and password). When an individual executes a series of signings during a single continuous period of controlled system access, the first signing is executed using all electronic signature components; subsequent signings are executed using at least one electronic signature component. When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing is executed using all of the electronic signature components. 2. Are administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals (i.e., system administrator and supervisor).
Level 2 Control Standard Mapping:	21 CFR Part 11.200(a) 21 CFR Part 11.3 21 CFR Part 11.300 AICPA 2017 CC6.6 CIS CSC v7.1 16.5 CMSRs v3.1 IA-05 (HIGH) CMSRs v3.1 IA-05 (HIGH; MOD) CMSRs v3.1 IA-05(01) (HIGH; MOD) FedRAMP IA-5 FedRAMP IA-5(6) FedRAMP IA-5(7) IRS Pub 1075 v2016 9.3.7.5 ISO/IEC 27002:2013 9.2.4 ISO/IEC 27799:2016 9.2.4 MARS-E v2 IA-5 MARS-E v2 IA-5(7) NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.DS-2 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 IA-5(1)c[HML]{0} NRS 603A.215.1 PCI DSS v3.2.1 8.2.1

Level CIS Implementation Requirements

Level CIS Implementation:	Before deploying any new devices in a networked environment, the organization changes all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.

Level CMS Implementation Requirements

Level CMS Implementation:	The organization enforces the following minimum password requirements (User/Privileged/Process [acting on behalf of a User]): 1. MinimumPasswordAge = one day; 2. MaximumPasswordAge = 60 days; 3. MinimumPasswordLength = Minimum length of 8 characters for regular user passwords, and minimum length of 15 characters for administrators or privileged user passwords; 4. PasswordComplexity = minimum (three for High or one for Moderate or Low) character(s) from the four-character categories (A-Z, a-z, 0-9, special characters; and 5. PasswordHistorySize = 12 passwords for High or six passwords for Moderate or Low systems.

	PIV compliant access cards are valid for no longer than five years; and PKI certificates issued in accordance with the Federal PKI Common Policy are valid for no longer than three years. Organizations ensure non-standard account-authenticators are managed in accordance with the CMS Risk Management Handbook (RMH), Volume III, Standard 4.3, Non-Standard Authenticator Management.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The organization enforces the following minimum password requirements: 1. Minimum Password Length = eight characters; 2. Password Complexity =none; and The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	The information system must, for password-based authentication: 1. Enforce password minimum lifetime restriction of one day; 2. Enforce non-privileged account passwords to be changed at least every 90 days; and 3. Enforce privileged account passwords to be changed at least every 60 days.

Level HIX Implementation Requirements

Level HIX Implementation:	PKI certificates issued in accordance with the Federal PKI Common Policy are valid for no longer than three years. The organization enforces the following minimum password requirements (User/Privileged/Process [acting on behalf of a User]): 1. Minimum Password Age = 1/1/1; 2. Maximum Password Age = 60/60/180; 3. Minimum Password Length = 8/8/15; 4. Password Complexity = User/Privileged Accounts: Eight characters; at least one numeric and at least one special character; a mixture of at least one uppercase and at least one lowercase letter; and 5. Password History Size = 24/24/24.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The information systems follow the direction in the applicable baseline configurations per CM-6, or if more stringent, the information system, for password-based authentication: (i) prohibits the use of dictionary names or words; (ii) meets or exceeds enforcement of the following minimum password requirements: (a) MinimumPasswordAge = one [1] day; (b) MaximumPasswordAge = sixty [60] days; (c) MinimumPasswordLength = Minimum length of eight [8] characters for regular user passwords, and minimum length of fifteen [15] characters for administrators or privileged user passwords; (d) PasswordComplexity = minimum (one [1] for Moderate) character(s) from the four [4] character categories (A-Z, a-z, 0-9, special characters); and (e) PasswordHistorySize = six [6] passwords for Moderate. (iii) The minimum length (MinimumPasswordLength) for administrators or

	privileged users is fifteen [15] characters; (iv) if the operating environment enforces a minimum of number of changed characters when new passwords are created, set the value at six [6] for Moderate systems; (v) stores and transmits only encrypted representations of passwords; and (vi) allows the use of a temporary password for system logons with an immediate change to a permanent password.

Level PCI	Implementation Requirements
Level PCI Implementation:	Passwords/passphrases require a minimum length of at least seven characters and contain both numeric and alphabetic characters. Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above. The organization: 1. changes user passwords/passphrases at least once every 90 days; 2. does not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used; and 3. sets passwords/passphrases for first-time use and upon reset to a unique value for each user and change immediately after the first use.

Level Supplemental Requirements	Implementation Requirements
Level Supplemental Requirements Implementation:	Authentication credentials are provided using a secure method.

Control Reference: 01.e Review of User Access Rights

Control Specification:	All access rights shall be regularly reviewed by management via a formal documented process. *Required for HITRUST Certification CSF v9.6
Factor Type:	System
Topics:	Audit and Accountability; Monitoring; User Access

Level 1	Implementation Requirements
Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to NY OHIP Moderate-Plus Security Baseline Subject to State of Massachusetts Data Protection Act Subject to Texas Health and Safety Code
Level 1 Implementation:	The following procedures are carried out to ensure the regular review of access rights by management: 1. user's access rights are reviewed after any changes, such as promotion, demotion, or termination of employment, or other arrangement with a workforce member ends; and 2. user's access rights are reviewed and re-allocated when moving from one employment or workforce member arrangement to another within the same organization.

Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 201 CMR 17.03(2)(h) 21 CFR Part 11.10(d) CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CIS CSC v7.1 16.7 CMSRs v3.1 PS-05 (HIGH; MOD) CSA CCM v3.0.1 IAM-10 FedRAMP PS-5 FFIEC IS v2016 A.6.20(c) FFIEC IS v2016 A.6.22(c) FFIEC IS v2016 A.6.8(c) ISO/IEC 27001:2013 A.9.2.6 ISO/IEC 27002:2013 9.2.5 ISO/IEC 27799:2016 9.2.5 MARS-E v2 PS-5 NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.AC-4 NY DOH SSP v3.1 AC-6(7).NYS3[MN]-2

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Is the system(s) accessible from the Internet? Yes Number of interfaces to other systems 25 to 75
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 4 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Supplemental Requirements Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The organization maintains a documented list of authorized users of information assets. In addition: 1. all types of accounts are reviewed at least every 90 days; 2. critical system accounts are reviewed at least every 60 days; 3. user's access rights are reviewed at least every 90 days; 4. changes to access authorizations are reviewed at least every 90 days; and 5. authorizations for special privileged access rights are reviewed at least every 60 days.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(d) CIS CSC v7.1 16.7 CMMC v1.0 AC.4.025-0 CMSRs v3.1 AC-02 (HIGH; MOD) COBIT 5 DS5.3 COBIT 5 DS5.4 COBIT 5 DSS05.04 FedRAMP AC-2 FedRAMP CM-5(5) FFIEC IS v2016 A.6.20(d) FFIEC IS v2016 A.6.22(c) IRS Pub 1075 v2016 9.3.1.2

	ISO/IEC 27002:2013 9.2.5 ISO/IEC 27799:2016 9.2.5 MARS-E v2 AC-2 NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST SP 800-53 R4 AC-2j[HML]{2} NIST SP 800-53 R4 CM-5(5)b[S]{0} NY DOH SSP v3.1 AC-2d[M]-1 NY DOH SSP v3.1 AC-2j[M]-0 NY DOH SSP v3.1 AC-6(7).NYS1[MN]-0 NY DOH SSP v3.1 AC-6(7).NYS2[MN]-0 NY DOH SSP v3.1 AC-6(7).NYS3[MN]-1 NY DOH SSP v3.1 CM-5(5).IS1[M]-3 NY DOH SSP v3.1 CM-5(5)b[MN]-0 SR v6.4 19d-0

Level CIS Implementation Requirements

Level CIS Implementation:	The organization reviews all system accounts and disables any account that cannot be associated with a business process and owner. The organization monitors for and notifies the user or user's manager of dormant accounts; and disables such accounts if not needed, or documents and monitors exceptions (e.g., vendor maintenance accounts needed for system recovery or continuity operations). The organization also requires that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators are then required to disable accounts that are not assigned to valid workforce members.

Level HIE Implementation Requirements

Level HIE Implementation:	HIEs, for all employees and for all employees of connecting organizations, review users with access and the appropriateness of each user’s role every 90 days. Any discrepancies are remediated immediately following the review.

Level HIX Implementation Requirements

Level HIX Implementation:	The organization inspects privileged accounts (e.g., administrator groups, root accounts, and other system-related accounts) on demand, and at least once every 14 days to ensure unauthorized accounts have not been created. Privileged user roles associated with applications are inspected every 30 days.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The organization reviews the privileges assigned to defined personnel or roles defined in the applicable security plan every ninety [90] days to validate the need for such privileges; and reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

Objective Name: 01.03 User Responsibilities

Control Objective:	To prevent unauthorized user access, and compromise or theft of information and information assets.

Control Reference: 01.f Password Use

Control Specification:	Users shall be made aware of their responsibilities for maintaining effective access controls and shall be required to follow good security practices in the selection and use of passwords and security of equipment.
Factor Type:	Organizational
Topics:	Authentication; Awareness and Training; Password Management

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to Joint Commission Accreditation Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (Supplemental) Subject to PCI Compliance Subject to State of Massachusetts Data Protection Act Subject to Texas Health and Safety Code Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	Users are made aware of the organization's password policies and requirements to: 1. keep passwords confidential; 2. avoid keeping a record (e.g., paper, software file or hand-held device) of passwords, unless this can be stored securely, and the method of storing has been approved; 3. change passwords whenever there is any indication of possible system or password compromise; 4. not share individual user accounts or passwords; 5. not provide their password to anyone for any reason (to avoid compromising their user credentials through social engineering attacks); 6. not use the same password for business and non-business purposes; and 7. select quality passwords (see requirements in 01.d). If users need to access multiple services, systems, or platforms, and are required to maintain multiple separate passwords, they are advised that they may use a single, quality password for all services where the user is assured that a reasonable level of protection has been established for the storage of the password within each service, system, or platform.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 201 CMR 17.04(1)(b) 201 CMR 17.04(1)(e) CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 1 153: Eligibility and Benefits Connectivity Rule v1.1.0 Subsection 5.2 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 IA-05 (HIGH; MOD) FedRAMP IA-5 IRS Pub 1075 v2016 9.3.7.5 ISO/IEC 27002:2013 9.3.1 ISO/IEC 27799:2016 9.3.1 MARS-E v2 IA-5 NIST Cybersecurity Framework v1.1 PR.AC-1

	NIST Cybersecurity Framework v1.1 PR.AT-1 NIST SP 800-53 R4 IA-5(8)[S]{0} NRS 603A.215.1 PCI DSS v3.2.1 8.2.5 PCI DSS v3.2.1 8.2.6 PCI DSS v3.2.1 8.4 TJC IM.02.01.03, EP 5

Control Reference: 01.g Unattended User Equipment

Control Specification:	Users shall ensure that unattended equipment has appropriate protection.
Factor Type:	Organizational
Topics:	Awareness and Training; Media and Assets

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline
Level 1 Implementation:	All users are made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users are advised to: 1. terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism (e.g., a password protected screen saver); 2. log-off mainframe computers, servers, and office PCs when the session is finished (e.g., not just switch off the PC screen or terminal); 3. secure PCs or terminals from unauthorized use by a key lock or an equivalent control (e.g., password access) when not in use. The organization safeguards information system output devices (e.g., printers) to help prevent unauthorized individuals from obtaining the output.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 AC-11 (HIGH; MOD) CMSRs v3.1 PE-05 (HIGH; MOD) CSA CCM v3.0.1 HRS-10 FedRAMP PE-5 IRS Pub 1075 v2016 4.3.2 IRS Pub 1075 v2016 9.3.1.9 IRS Pub 1075 v2016 9.3.11.5 ISO/IEC 27002:2013 11.2.8 ISO/IEC 27799:2016 11.2.8 MARS-E v2 AC-11 MARS-E v2 PE-5 NIST Cybersecurity Framework v1.1 PR.AC-2 NIST Cybersecurity Framework v1.1 PR.AT-1 NIST Cybersecurity Framework v1.1 PR.PT-2 NIST SP 800-53 R4 PE-5(1)[S]{0} NIST SP 800-53 R4 PE-5(2)a[S]{0}

	NIST SP 800-53 R4 PE-5[HM]{0} NY DOH SSP v3.1 PE-18[HN]-3 NY DOH SSP v3.1 PE-5[M]-0

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation:	Output from printers and fax machines is in a controlled area and secured when not in use. Physical access to monitors displaying FTI is controlled to prevent unauthorized access to the display output.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation:	To mitigate attacks against encryption keys, when outside of State facilities, SE laptops and third-party laptops that access or contain SE PPSI must be powered down (i.e., shut down or hibernated) when unattended.

Control Reference: 01.h Clear Desk and Clear Screen Policy

Control Specification:	A clear desk policy for papers and removable storage media and a clear screen policy for information assets shall be adopted. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Awareness and Training; Data Loss Prevention; Documentation and Records; Media and Assets; Policies and Procedures

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to HITRUST De-ID Framework Requirements Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to Texas Health and Safety Code
Level 1 Implementation:	A clear desk policy for papers and removable storage media and a clear screen policy for information assets are developed and adopted and communicated to all users. The clear desk and clear screen policy take into account the information classifications, legal and contractual requirements, and the corresponding risks and cultural aspects of the organization. The following practices are established: 1. covered or critical business information (e.g., on paper or on electronic storage media) is locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated; 2. computers and terminals are left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism that conceals information previously visible on the

	display when unattended, and are protected by key locks, passwords, or other controls when not in use; 3. incoming and outgoing mail points and unattended facsimile machines are protected; 4. unauthorized use of photocopiers and other reproduction technology (e.g., scanners, digital cameras) is prevented; 5. documents containing covered or classified information are removed from printers, copiers, and facsimile machines immediately; and 6. when transporting documents with covered information within facilities and through inter-office mail, information is not visible through envelope windows, and envelopes are marked according to the information's classification level (e.g., "Confidential").
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 AC-11 (HIGH; MOD) CMSRs v3.1 MP-03 (HIGH; MOD) CSA CCM v3.0.1 HRS-11 De-ID Framework v1 Physical Security: General HITRUST IRS Pub 1075 v2016 9.3.1.9 IRS Pub 1075 v2016 9.3.10.3 ISO/IEC 27002:2013 11.2.9 ISO/IEC 27002:2013 8.2.3 ISO/IEC 27799:2016 11.2.9 ISO/IEC 27799:2016 8.2.3 MARS-E v2 AC-11 MARS-E v2 MP-3 NIST Cybersecurity Framework v1.1 PR.PT-2

Objective Name: 01.04 Network Access Control

Control Objective:	To prevent unauthorized access to networked services.

Control Reference: 01.i Policy on the Use of Network Services

Control Specification:	Users shall only be provided with access to internal and external network services that they have been specifically authorized to use. Authentication and authorization mechanisms shall be applied for users and equipment.
Factor Type:	Organizational
Topics:	Authentication; Authorization; Network Segmentation; User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to NY OHIP Moderate-Plus Security Baseline
Level 1 Implementation:	The organization specifies the networks and network services to which users are authorized access.
Level 1	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi)

Control Standard Mapping:	CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CIS CSC v7.1 13.4 CMSRs v3.1 AC-01 (HIGH; MOD) CRR v2016 CM:G2.Q8 IRS Pub 1075 v2016 9.3.1.1 ISO/IEC 27001:2013 9.1.2 ISO/IEC 27799:2016 9.1.2 MARS-E v2 AC-1 NIST Cybersecurity Framework v1.1 PR.PT-3 NY DOH SSP v3.1 AC-2i2[M]-1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 1 Subject to Community Supplemental Requirements 002 Subject to FedRAMP Certification Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The organization: 1. determines who is allowed to access which network and networked services (see 01.i, level 1); and 2. specifies the means that can be used to access networks and network services (e.g., the conditions for allowing access to a remote system). At a minimum, the organization manages all enterprise devices remotely logging into the internal network, with remote control of their configuration, installed software, and patch levels. The organization also publishes minimum security standards for access to the enterprise network by third-party devices (e.g., subcontractors/vendors), and performs a security scan before allowing access. The use of network services is consistent with the organization's business access control requirements. Use of external information systems is managed effectively including:

	1. information systems or components of information systems that are outside of the accreditation boundary established by the organization are identified as external information systems including: i. information systems or components of information systems for which the organization typically has no direct control over the application of required security controls, or the assessment of security control effectiveness are identified as external information systems; ii. personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants) are identified as external information systems; and iii. privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports) are identified as external information systems. 2. authorized individuals are prohibited from using an external information system to access the information system or to process, store or transmit organization-controlled information except in situations where the organization: i. can verify the employment of required security controls on the external system as specified in the organization's information security policy and system security plan; or ii. has approved information system connection or processing agreements with the organizational entity hosting the external information system. The organization identifies ports, services, and similar applications (e.g., protocols) necessary for business and provides the rationale or identifies compensating controls implemented for those protocols considered to be insecure.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC6.1 CMMC v1.0 AC.1.003-2 CMSRs v3.1 AC-20 (HIGH; MOD) CMSRs v3.1 CM-07 (HIGH; MOD) CRR v2016 CM:G2.Q8 CSA CCM v3.0.1 IAM-09 CSA CCM v3.0.1 IVS-06 CSR002 v2018 11.2-3-2 FedRAMP AC-20 FedRAMP CM-7 FFIEC IS v2016 A.6.7(a) FFIEC IS v2016 A.6.7(b) FFIEC IS v2016 A.6.7(c) IRS Pub 1075 v2016 9.3.1.15 IRS Pub 1075 v2016 9.3.5.7 ISO/IEC 27002:2013 9.1.2 ISO/IEC 27799:2016 9.1.2 MARS-E v2 AC-20 MARS-E v2 CM-7 NIST 800-171 r2 3.1.20-2 NIST Cybersecurity Framework v1.1 DE.AE-1 NIST Cybersecurity Framework v1.1 ID.AM-4 NIST Cybersecurity Framework v1.1 PR.IP-1 NIST Cybersecurity Framework v1.1 PR.PT-3 NIST SP 800-53 R4 AC-17(6)[S]{2} NIST SP 800-53 R4 AC-17a[HML]{4} NIST SP 800-53 R4 AC-20(4)[S]{2} NY DOH SSP v3.1 AC-20(1)[M]-0 NY DOH SSP v3.1 AC-20(1)a[M]-0 NY DOH SSP v3.1 AC-20(1)b[M]-0

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The service provider uses the Center for Internet Security guidelines (Level 1) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if United States Government Configuration Baseline (USGCB) is not available.

Control Reference: 01.j User Authentication for External Connections

Control Specification:	Appropriate authentication methods shall be used to control access by remote users. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Authentication; Authorization; Third-parties and Contractors; User Access; Network Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 2 Subject to CMMC Level 3 Subject to FTC Red Flags Rule Subject to HITRUST De-ID Framework Requirements Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Supplemental Requirements
Level 1 Implementation:	Authentication of remote users is implemented using a password or passphrase and at least one of the following methods: 1. a cryptographic based technique; 2. biometric techniques; 3. hardware tokens; 4. software tokens; 5. a challenge/response protocol; or 6. certificate agents. The organization protects wireless access to systems containing sensitive information by authenticating users and devices. Remote access to business information across public networks only takes place after successful identification and authentication. Remote access by vendors and business partners (e.g., maintenance, reports, or other data access) is disabled unless specifically authorized by management. If remote maintenance is performed, the organization closely monitors and controls any activities, with immediate deactivation after use. Remote access to business partner accounts is also immediately deactivated after use. If encryption is not used for dial-up connections, the CIO or his/her designated representative must provide specific written authorization.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(3) 1 TAC § 390.2(a)(4)(A)(xi) 16 CFR Part § 681 Appendix A III(b) 21 CFR Part 11.10(d) AICPA 2017 CC6.1 CMMC v1.0 AC.3.012-2

	CMMC v1.0 MA.2.113-2 CMSRs v3.1 AC-17 (HIGH; MOD) CMSRs v3.1 AC-18 (HIGH; MOD) CMSRs v3.1 AC-18(01) (HIGH; MOD) CMSRs v3.1 IA-02 (HIGH; MOD) CMSRs v3.1 IA-08 (HIGH; MOD) CMSRs v3.1 IA-08(01) (HIGH; MOD) CMSRs v3.1 IA-08(02) (HIGH; MOD) CMSRs v3.1 IA-08(03) (HIGH; MOD) CMSRs v3.1 IA-08(04) (HIGH; MOD) CMSRs v3.1 MA-04 (HIGH; MOD) CRR v2016 CCM:G2.Q11 De-ID Framework v1 Remote Access: Applicability FedRAMP AC-17 FedRAMP AC-18 FedRAMP AC-18(1) FedRAMP IA-2 FedRAMP MA-4 FFIEC IS v2016 A.6.21(e) FFIEC IS v2016 A.6.23 FFIEC IS v2016 A.6.24 HITRUST IRS Pub 1075 v2016 9.3.1.12 IRS Pub 1075 v2016 9.3.1.13 IRS Pub 1075 v2016 9.3.7.2 IRS Pub 1075 v2016 9.3.9.4 MARS-E v2 AC-17 MARS-E v2 AC-18 MARS-E v2 AC-18(1) MARS-E v2 IA-2 MARS-E v2 IA-8 MARS-E v2 MA-4 NIST 800-171 r2 3.1.17-2 NIST 800-171 r2 3.7.5-2 NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.AC-3 NIST Cybersecurity Framework v1.1 PR.MA-2 NIST Cybersecurity Framework v1.1 PR.PT-4 NIST SP 800-53 R4 AC-17(4)b[HM]{0} NIST SP 800-53 R4 MA-4(7)[S]{0} NIST SP 800-53 R4 MA-4e[HML]{0} NRS 603A.215.1 NY DOH SSP v3.1 AC-18(1)[M]-2 NY DOH SSP v3.1 IA-2(11)[M]-3 NY DOH SSP v3.1 MA-4d[M]-0 PCI DSS v3.2.1 12.3.9 PCI DSS v3.2.1 8.1.5 PCI DSS v3.2.1 8.3.2 SR v6.4 13-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to NIST SP 800-53 R4 (Supplemental)

Level 2 Implementation:	Level 1 plus: Authentication of remote users is implemented via virtual private network (VPN) solutions that support a cryptographic-based technique, hardware tokens, or a challenge/response protocol. Dedicated private lines may also be used to provide assurance of the source of connections. Control all remote access through a limited number of managed access control points. Periodic monitoring is implemented to ensure that installed equipment does not include unanticipated dial-up capabilities. Require callback capability with re-authentication to verify connections from authorized locations. For application systems and turnkey systems that require the vendor to log-on, the vendor is assigned a User ID and password and must enter the network through the standard authentication process. Access to such systems is authorized and logged. User IDs assigned to vendors will be reviewed in accordance with the organization's access review policy, at a minimum annually. Node authentication, including cryptographic techniques (e.g., machine certificates), are required for authenticating groups of remote users where they are connected to a secure, shared computer facility. This is part of several VPN based solutions. The organization requires all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems, e.g., from an alternate work location or to sensitive information via a web portal) to use two-factor authentication.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CIS CSC v7.1 12.11 CMSRs v3.1 AC-02 (HIGH; MOD) CMSRs v3.1 AC-17 (HIGH; MOD) CMSRs v3.1 AC-17(02) (HIGH; MOD) CMSRs v3.1 AC-17(03) (HIGH; MOD) CMSRs v3.1 CM-02 (HIGH; MOD) CMSRs v3.1 CM-02(02) (HIGH) CMSRs v3.1 IA-08 (HIGH; MOD) CMSRs v3.1 IA-08(01) (HIGH; MOD) CMSRs v3.1 IA-08(02) (HIGH; MOD) CMSRs v3.1 IA-08(03) (HIGH; MOD) CMSRs v3.1 IA-08(04) (HIGH; MOD) FedRAMP AC-17 FedRAMP AC-17(2) FedRAMP AC-17(3) FedRAMP AC-2 FFIEC IS v2016 A.6.23 FFIEC IS v2016 A.6.24 IRS Pub 1075 v2016 9.3.1.12 IRS Pub 1075 v2016 9.3.1.2 IRS Pub 1075 v2016 9.3.7.8 MARS-E v2 AC-17 MARS-E v2 AC-17(2) MARS-E v2 AC-17(3) MARS-E v2 AC-2 MARS-E v2 IA-5(11) MARS-E v2 IA-8 MARS-E v2 ICM-2 NIST Cybersecurity Framework v1.1 DE.CM-1 NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.AC-3 NIST Cybersecurity Framework v1.1 PR.DS-2 NIST Cybersecurity Framework v1.1 PR.PT-4 NIST SP 800-53 R4 CP-13[S]{0} NIST SP 800-53 R4 MA-4(4)b[S]{1}

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions

	Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to Banking Requirements Subject to CMMC Level 2 Subject to CMMC Level 3 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: The information system monitors and controls remote access methods. The execution of privileged commands and access to security-relevant information via remote access is only authorized for compelling operational needs and rationale documented.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMMC v1.0 AC.2.013-0 CMMC v1.0 AC.3.021-0 CMSRs v3.1 AC-06(03) (HIGH) CMSRs v3.1 AC-17(01) (HIGH; MOD) CMSRs v3.1 AC-17(04) (HIGH; MOD) FedRAMP AC-17(1) FedRAMP AC-17(4) FFIEC IS v2016 A.6.23 FFIEC IS v2016 A.6.24 IRS Pub 1075 v2016 9.4.13 IRS Pub 1075 v2016 9.4.18 MARS-E v2 AC-17(1) MARS-E v2 AC-17(2) NIST 800-171 r2 3.1.12-0 NIST 800-171 r2 3.1.15-0 NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.AC-3 NIST Cybersecurity Framework v1.1 PR.DS-2 NIST Cybersecurity Framework v1.1 PR.PT-4 NIST SP 800-53 R4 AC-17(1)[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 AC-17(1)[M]-1 NY DOH SSP v3.1 AC-17.IS4a[M]-0 NY DOH SSP v3.1 AC-17[M]-2 NY DOH SSP v3.1 AC-17[M]-3 NY DOH SSP v3.1 AC-17a[M]-1 NY DOH SSP v3.1 AC-17b[M]-0

Level CIS Implementation Requirements

Level CIS Implementation:	The organization requires all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems, e.g., from an alternate work location

	or to sensitive information via a web portal) to encrypt data in transit and use two-factor authentication.

Level CMMC Implementation Requirements	
Level CMMC Implementation:	The system restricts remote network access based on organizational defined risk factors, e.g., time of day, location of access, physical location, network connection state, and measured properties of the current user and role.

Level CMS Implementation Requirements	
Level CMS Implementation:	If e-authentication is implemented as a remote access solution or associated with remote access, refer to the Risk Management Handbook (RMH), Volume III, Standard 3.1, 'CMS Authentication Standards'.

Level Federal Implementation Requirements	
Level Federal Implementation:	The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies. The information system accepts only Federal Identity, Credential, and Access Management (FICAM)-approved third-party credentials. The organization employs only FICAM-approved information system components in information systems that authenticate non-organizational users and accept third-party credentials. The information system conforms to FICAM-issued profiles.

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation:	The organization provides the capability to expeditiously disconnect or disable remote access to the organizations system(s) within 15 minutes based on the criticality of missions/business functions and the need to eliminate immediate or future remote access to organizational information system(s). The information system uses only FICAM-approved components and conforms to FICAM-issued profiles, accepts only FICAM-approved third-party credentials, and accepts and electronically verifies PIV credentials from other federal organizations.

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation:	For remote access to FTI, encrypted modems and/or Virtual Private Networks (VPN) are required for every workstation and a smart card (microprocessor) for every user. Smart cards must have both identification and authentication features and must provide data encryption as well. The agency authorizes, documents, and monitors all wireless access to the information system. WLAN infrastructure that receives, processes, stores, or transmits FTI must comply with the IEEE 802.11i security standard and perform mutual authentication for all access to FTI via an 802.1X extensible authentication protocol (EAP).

	Users who access FTI remotely in a Virtual Desktop Infrastructure (VDI) must use multi-factor authentication to validate their identities.

Level HIX Implementation Requirements	
Level HIX Implementation:	The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation:	Require callback capability with re-authentication to verify connections from authorized locations when the Medicare Data Communications Network (MDCN) or Multi-Protocol Label Switching (MPLS) service network cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor will be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems will be authorized and logged. User IDs assigned to vendors will be recertified within every [365] days.

Level PCI Implementation Requirements	
Level PCI Implementation:	The organization incorporates multi-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third-parties (including vendor access for support and maintenance).

Control Reference: 01.k Equipment Identification in Networks

Control Specification:	Automatic equipment identification shall be used as a means to authenticate connections from specific locations and equipment.
Factor Type:	System
Topics:	Authentication; Communications and Transmissions; Media and Assets; Network Security

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	An identifier in or attached to the equipment is used to indicate whether this equipment is permitted to connect to the network. These identifiers clearly indicate to which network the equipment is permitted to connect, if more than one network exists and particularly if these networks are of differing sensitivity. Physical protection of the equipment is required to maintain the security of the equipment identifier. The identifier is stored and transported in an encrypted format to protect it from unauthorized access.

Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC6.1 CMSRs v3.1 IA-03 (HIGH; MOD) CMSRs v3.1 IA-05 (HIGH; MOD) COBIT 5 DS5.7 COBIT 5 DSS05.05 CSA CCM v3.0.1 DCS-03 FedRAMP IA-3 FedRAMP IA-5 IRS Pub 1075 v2016 9.3.7.3 IRS Pub 1075 v2016 9.3.7.5 MARS-E v2 IA-3 MARS-E v2 IA-5 NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.AC-2 NIST Cybersecurity Framework v1.1 PR.DS-1

Control Reference: 01.l Remote Diagnostic and Configuration Port Protection

Control Specification:	Physical and logical access to diagnostic and configuration ports shall be controlled. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Authorization; Media and Assets; Physical and Facility Security; Network Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation:	Access to network equipment is physically protected (e.g., a router must be stored in a room that is only accessible by authorized employees or contractors).
Level 1 Control Standard Mapping:	CMSRs v3.1 PE-03(01) (HIGH) NIST Cybersecurity Framework v1.1 PR.AC-2 NIST Cybersecurity Framework v1.1 PR.PT-3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	

Level 2 Regulatory Factors:	Subject to CMMC Level 3 Subject to FISMA Compliance Subject to NIST 800-171 Derived Level
Level 2 Implementation:	Level 1 plus: Controls for the access to diagnostic and configuration ports include the use of a key lock. Ports, services, and similar applications installed on a computer or network systems, which are not specifically required for business functionality, are disabled, or removed. Supporting procedures to control physical access to the port are implemented including ensuring that diagnostic and configuration ports are only accessible by arrangement between the manager of the computer service and the hardware/software support personnel requiring access.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC6.1 CIS CSC v7.1 9.2 CMMC v1.0 CM.3.068-1 CMSRs v3.1 CM-07 (HIGH; MOD) CMSRs v3.1 MA-04 (HIGH; MOD) CMSRs v3.1 MA-04(02) (HIGH; MOD) CMSRs v3.1 MA-04(03) (HIGH) COBIT 5 DS5.7 COBIT 5 DSS05.05 CSA CCM v3.0.1 IAM-03 CSA CCM v3.0.1 IVS-07 FedRAMP CM-7 FedRAMP MA-4 IRS Pub 1075 v2016 9.3.9.4 MARS-E v2 CM-7 MARS-E v2 MA-4 MARS-E v2 MA-4(2) MARS-E v2 MA-4(3) NIST 800-171 r2 3.4.7-1 NIST Cybersecurity Framework v1.1 PR.AC-2 NIST Cybersecurity Framework v1.1 PR.MA-1 NIST Cybersecurity Framework v1.1 PR.PT-3

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 4 Subject to FedRAMP Certification Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NY OHIP Moderate-Plus Security Baseline Subject to Supplemental Requirements Subject to the CMS Minimum Security Requirements (High)

Level 3 Implementation:	Level 2 plus: The organization reviews the information system within every 365 days to identify and disable unnecessary and non-secure functions, ports, protocols, and/or services. The organization disables Bluetooth and peer-to-peer networking protocols within the information system determined unnecessary (for which there is not a documented business need) or non-secure. The organization disables peer-to-peer wireless network capabilities on wireless clients. The organization identifies unauthorized software on the information system; employs an allow-all, deny-by-exception policy to prohibit the execution of known unauthorized software on the information system; and reviews and updates the list of unauthorized software periodically, but no less than annually.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CIS CSC v7.1 15.6 CIS CSC v7.1 9.3 CMMC v1.0 RM.4.151-0 CMSRs v3.1 CM-07 (HIGH; MOD) CMSRs v3.1 CM-07(01) (HIGH; MOD) CMSRs v3.1 CM-07(02) (HIGH; MOD) CMSRs v3.1 CM-07(05) (HIGH) FedRAMP CM-7 FedRAMP CM-7(5) IRS Pub 1075 v2016 9.3.5.7 IRS Pub 1075 v2016 9.4.9 MARS-E v2 CM-7 MARS-E v2 CM-7(1) NIST Cybersecurity Framework v1.1 DE.AE-1 NIST Cybersecurity Framework v1.1 ID.AM-2 NIST Cybersecurity Framework v1.1 ID.AM-3 NIST Cybersecurity Framework v1.1 PR.IP-1 NIST Cybersecurity Framework v1.1 PR.IP-3 NIST Cybersecurity Framework v1.1 PR.PT-3 NY DOH SSP v3.1 CM-7(1)c[M]-0 SR v6.4 6.6-0

Level CMS Implementation Requirements

Level CMS Implementation:	The organization identifies defined software programs authorized to execute on the information system, employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system, reviews and updates the list of authorized software programs no less often than every 72 hours, and receives automated updates from a trusted source. A list of specifically needed system services, ports, and network protocols will be maintained and documented in the security plan. If collaborative computing is authorized, the information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The organization reviews the information system at least monthly to identify and disables unnecessary and non-secure functions, ports, protocols, and/or services. The organization identifies defined software programs authorized to execute on the information system, employs automated mechanisms to prevent program execution in accordance with the list of authorized programs through a deny-all, permit-by-exception

	policy, and reviews and updates the list of authorized software programs within every 30 days. The organization employs automated mechanisms to scan the network continuously with a maximum five-minute delay in detection to detect the presence of unauthorized components/devices (including hardware, firmware, and software) into the information system; and disable network access by such components/devices and notify designated organizational officials.

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation:	Least functionality controls that must be in place that include disabling all unneeded network protocols, services, and assigning a dedicated static IP address to Multifunctional Devices (MFDs).

Control Reference: 01.m Segregation in Networks

Control Specification:	Groups of information services, users, and information systems should be segregated on networks. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Network Segmentation; Network Security

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 2 Subject to CMMC Level 4 Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to Supplemental Requirements
Level 1 Implementation:	Security gateways (e.g., a firewall) are used between the internal network, external networks (Internet and third-party networks), and any demilitarized zone (DMZ). An internal network perimeter is implemented by installing a secure gateway (e.g., a firewall) between two interconnected networks to control access and information flow between the two domains. This gateway is capable of enforcing security policies, be configured to filter traffic between these domains, and block unauthorized access in accordance with the organization's access control policy. Wireless networks are segregated from internal and private networks. The organization requires a firewall between any wireless network and the covered and/or confidential information system's environment.

Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC6.6 CMMC v1.0 AC.2.016-0 CMMC v1.0 AC.4.023-1 CRR v2016 CM:G2.Q2 CRR v2016 CM:G2.Q8 CSA CCM v3.0.1 DSI-02 CSA CCM v3.0.1 IVS-06 FFIEC IS v2016 A.6.10 IRS Pub 1075 v2016 9.4.10 ISO/IEC 27002:2013 13.1.3 ISO/IEC 27799:2016 13.1.3 NIST 800-171 r2 3.1.3-0 NIST Cybersecurity Framework v1.1 DE.AE-1 NIST Cybersecurity Framework v1.1 PR.AC-5 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST SP 800-53 R4 AC-4(6)[S]{0} NIST SP 800-53 R4 AC-4(7)[S]{0} NIST SP 800-53 R4 AC-4(8)[S]{0} NIST SP 800-53 R4 SC-7(21)[H]{0} NRS 603A.215.1 NY DOH SSP v3.1 AC-4[M]-1 PCI DSS v3.2.1 1.1 PCI DSS v3.2.1 1.1.4 SR v6.4 10.2-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 1 Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The criteria for segregation of networks into domains is based on the access control policy and access requirements, and also takes account of the relative cost and performance impact of incorporating suitable network routing or gateway technology. In addition, segregation of networks is based on the value and classification of information

	stored or processed in the network, levels of trust, or lines of business, in order to reduce the total impact of a service disruption. Networks are divided into separate logical network domains (e.g., an organization's internal network domains and external network domains) each protected by a defined security perimeter. A graduated set of controls is applied in different logical network domains to further segregate the network security environments (e.g., publicly-accessible systems; internal networks; critical assets; and key information security tools, mechanisms, and support components associated with system and security administration). Segregations of separate logical domains are achieved by restricting network access using virtual private networks for user groups within the organization. Networks are also segregated using network device functionality (e.g., IP switching). A baseline of network operations and expected data flows for users and systems is established and managed. Separate domains are then implanted by controlling the network data flows using routing/switching capabilities, including access control lists, according to applicable flow control policies. The domains are defined based on a risk assessment and the different security requirements within each of the domains. The organization implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks. To ensure proper separation, the organization verifies any server that is visible from the Internet or an untrusted network and, if it is not required for business purposes, moves it to an internal VLAN and gives it a private address. Organization uses a network segregated from production-level networks when migrating physical servers, applications, or data to virtualized servers. The organization manages the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC6.1 CIS CSC v7.1 11.7 CIS CSC v7.1 14.1 CIS CSC v7.1 15.10 CMMC v1.0 SC.1.176-0 CMSRs v3.1 AC-04 (HIGH; MOD) CMSRs v3.1 SC-07 (HIGH; MOD) CMSRs v3.1 SC-07(13) (HIGH) CMSRs v3.1 SC-32 (HIGH) COBIT 5 DS5.10 COBIT 5 DSS05.02 CRR v2016 CM:G2.Q2 CRR v2016 CM:G2.Q8 CSA CCM v3.0.1 IVS-09 CSA CCM v3.0.1 IVS-10 FedRAMP AC-4(21) FedRAMP SC-7 FedRAMP SC-7(13) FFIEC IS v2016 A.6.10 FFIEC IS v2016 A.6.17 IRS Pub 1075 v2016 9.3.1.4 IRS Pub 1075 v2016 9.3.16.5 IRS Pub 1075 v2016 9.4.11 IRS Pub 1075 v2016 9.4.13 IRS Pub 1075 v2016 9.4.14 IRS Pub 1075 v2016 9.4.15 IRS Pub 1075 v2016 9.4.18 IRS Pub 1075 v2016 9.4.5

	ISO/IEC 27002:2013 13.1.3 ISO/IEC 27799:2016 13.1.3 MARS-E v2 SC-32 MARS-E v2 SC-7 MARS-E v2 SC-7(13) NIST 800-171 r2 3.13.5-0 NIST Cybersecurity Framework v1.1 DE.AE-1 NIST Cybersecurity Framework v1.1 ID.AM-3 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.AC-5 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.IP-1 NIST Cybersecurity Framework v1.1 PR.PT-4 NIST SP 800-53 R4 AC-4(2)[S]{0} NIST SP 800-53 R4 AC-4(21)[S]{0} NIST SP 800-53 R4 SC-7(22)[S]{0} NIST SP 800-53 R4 SC-7b[HML]{0} NY DOH SSP v3.1 SC-7b[M]-0 PCI DSS v3.2.1 1.2

Level CIS Implementation Requirements

Level CIS Implementation:	Network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine is isolated from the organization's primary network and not be allowed Internet access. This machine is not used for reading email, composing documents, or surfing the Internet. Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incur higher risk for the organization. The organization manages the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices. The organization segments the network based on the label or classification level of the information stored on the servers, ensuring all sensitive information is located on separated VLANs. The organization creates separate virtual local area networks (VLANs) for BYOD systems or other untrusted devices (e.g., devices outside of the organization's control). Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.

Level CMS Implementation Requirements

Level CMS Implementation:	The organization partitions the information system into defined information system components (defined in the applicable security plan) residing in separate physical domains or environments based on defined circumstances (defined in the applicable security plan) for physical separation of components.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	To use an Integrated Voice Response (IVR) system that provides FTI over the telephone to a customer, the agency must ensure the LAN segment where the IVR system resides is firewalled (segmented) to prevent direct access from the Internet to the IVR system. To use FTI in a SAN environment, the agency must ensure FTI is segregated from other agency data within the SAN environment.

	To use Virtual Desktop Infrastructure (VDI) to provide FTI to a customer, the agency muse ensure VDI components are segregated so that boundary protections can be implemented, and access controls are granularized. To use a virtual environment that receives, processes, stores or transmits FTI, separation between VMs must be enforced, and functions that allow one VM to share data with the hypervisor or another VM, such as clipboard sharing or shared disks, must be disabled. To use a VoIP network that provides FTI to a customer, VoIP traffic that contains FTI is segmented off from non-VoIP traffic through segmentation. If complete segmentation is not feasible, the agency must have compensating controls in place and properly applied that restrict access to VoIP traffic that contains FTI. VoIP-ready firewalls must be used to filter VoIP traffic on the network. To use FTI in an 802.11 WLAN, the agency must architect the WLAN environment to provide logical separation between WLANs with different security profiles, and from the wired LAN.

Level HIX Implementation Requirements

Level HIX Implementation:	The organization partitions the information system into defined information system components (defined in the applicable security plan) residing in separate physical domains (or environments), based on defined circumstances (defined in the applicable security plan) for physical separation of components.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The information system routes all remote accesses through a limited number of managed access control points. The organization must identify acceptable network access control points (e.g., connections standardized through the TIC initiative). Systems processing, storing, or transmitting PII (to include PHI): In any situation where personally identifiable information (PII) is present, PII must be stored on a logical or physical partition separate from the applications and software partition.

Control Reference: 01.n Network Connection Control

Control Specification:	For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Network Segmentation; User Access; Network Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	

Level 1 Regulatory Factors:	Subject to CMMC Level 2 Subject to CMMC Level 3 Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to State of Massachusetts Data Protection Act
Level 1 Implementation:	At managed interfaces, network traffic is denied by default and allowed by exception (i.e., deny all, permit by exception). The organization restricts the ability of users to connect to the internal network in accordance with the access control policy and the requirements of the business applications.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 201 CMR 17.04(6) CMMC v1.0 AC.2.015-0 CMMC v1.0 SC.3.183-0 CMSRs v3.1 SC-07 (HIGH; MOD) CMSRs v3.1 SC-07(05) (HIGH; MOD) CRR v2016 CM:G2.Q2 CRR v2016 CM:G2.Q8 FedRAMP SC-7 FedRAMP SC-7(5) IRS Pub 1075 v2016 9.3.16.5 MARS-E v2 SC-7 MARS-E v2 SC-7(5) NIST 800-171 r2 3.1.14-0 NIST 800-171 r2 3.13.6-0 NIST Cybersecurity Framework v1.1 DE.AE-1 NIST Cybersecurity Framework v1.1 PR.AC-3 NIST Cybersecurity Framework v1.1 PR.AC-5 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.PT-4 NIST SP 800-53 R4 SC-7(11)[S]{0} NIST SP 800-53 R4 SC-7(5)[HM]{0} NRS 603A.215.1 NY DOH SSP v3.1 SC-7(5)[M]-0 PCI DSS v3.2.1 1.2.1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to CMMC Level 1 Subject to CMMC Level 3 Subject to Community Supplemental Requirements 002 Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance

	Subject to HITRUST De-ID Framework Requirements Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Basic Level Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Supplemental Requirements Subject to the CMS Minimum Security Requirements (High) Subject to the EU GDPR
Level 2 Implementation:	Level 1 plus: The connection capability of users is restricted through network gateways (e.g., a firewall) that filter traffic by means of pre-defined tables or rules. Restrictions are applied to: 1. messaging (e.g., electronic mail); 2. file transfer (e.g., peer-to-peer, FTP); 3. interactive access (e.g., where a user provides input to the system); and 4. common Windows applications. Review exceptions to the traffic flow policy within every 365 days or implementation of major new systems. Linking network access rights to certain times of day or dates is implemented. The organization limits the number of external network connections to the information system (e.g., prohibiting desktop modems) to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. The organization: 1. implements a managed interface for each external telecommunication service, i.e., transmissions of data to or from other entities external to the secure site, including to other secure sites using networks or any other communications resources outside of the physical control of the secure site to transmit information; 2. establishes a traffic flow policy for each managed interface; 3. employs security controls as needed to protect the confidentiality and integrity of the information being transmitted; 4. documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; 5. reviews exceptions to the traffic flow policy within every 365 days; and 6. removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need. Remote devices that have established a non-remote connection are prevented from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CIS CSC v7.1 16.5 CMMC v1.0 SC.1.175-1 CMMC v1.0 SC.3.184-0 CMSRs v3.1 AC-02(11) (HIGH) CMSRs v3.1 AC-17(03) (HIGH; MOD) CMSRs v3.1 SC-07(03) (HIGH; MOD)

	CMSRs v3.1 SC-07(04) (HIGH; MOD) CMSRs v3.1 SC-07(07) (HIGH; MOD) CMSRs v3.1 SC-07(08) (HIGH) CMSRs v3.1 SC-08 (HIGH; MOD) COBIT 5 DS5.10 COBIT 5 DSS05.02 CRR v2016 CM:G2.Q2 CRR v2016 CM:G2.Q4 CRR v2016 CM:G2.Q8 CSA CCM v3.0.1 IVS-06 CSA CCM v3.0.1 IVS-09 CSR002 v2018 11.2-1-3 De-ID Framework v1 Transmission Encryption: Policies FedRAMP AC-17 FedRAMP AC-17(3) FedRAMP SC-7(3) FedRAMP SC-7(4) FedRAMP SC-7(7) FedRAMP SC-8 IRS Pub 1075 v2016 9.3.1.12 IRS Pub 1075 v2016 9.3.1.4 IRS Pub 1075 v2016 9.3.16.5 IRS Pub 1075 v2016 9.4.10 IRS Pub 1075 v2016 9.4.16 IRS Pub 1075 v2016 9.4.17 MARS-E v2 AC-17 MARS-E v2 AC-17(3) MARS-E v2 SC-7(3) MARS-E v2 SC-7(4) MARS-E v2 SC-7(7) MARS-E v2 SC-7(8) MARS-E v2 SC-8 NIST 800-171 r2 3.13.1-1 NIST 800-171 r2 3.13.7-0 NIST Cybersecurity Framework v1.1 DE.AE-1 NIST Cybersecurity Framework v1.1 DE.CM-1 NIST Cybersecurity Framework v1.1 PR.AC-5 NIST Cybersecurity Framework v1.1 PR.DS-2 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.IP-3 NIST Cybersecurity Framework v1.1 PR.PT-4 NIST SP 800-53 R4 AU-5(3)[S]{1} NIST SP 800-53 R4 CA-3(1)[S]{0} NIST SP 800-53 R4 CA-3(3)[S]{0} NIST SP 800-53 R4 SC-7(4)a[HM]{0} NIST SP 800-53 R4 SC-7(4)d[HM]{0} NIST SP 800-53 R4 SC-7(4)e[HM]{0} NIST SP 800-53 R4 SC-7(7)[HM]{0} NIST SP 800-53 R4 SC-7c[HML]{0} NY DOH SSP v3.1 SC-7(3)[M]-0 NY DOH SSP v3.1 SC-7(4)a[M]-0 NY DOH SSP v3.1 SC-7(4)b[M]-0 NY DOH SSP v3.1 SC-7(4)d[M]-0 NY DOH SSP v3.1 SC-7(4)e[M]-0 NY DOH SSP v3.1 SC-7(7)[M]-0 NY DOH SSP v3.1 SC-7c[M]-0 PMI DSP Framework PR.DS-1 SR v6.4 42.1-0

Level CMS Implementation Requirements

Level CMS Implementation:	The information system routes all user-initiated internal communications traffic to untrusted external networks through authenticated proxy servers at managed interfaces.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The information system routes all user-initiated internal communications traffic to untrusted external networks through authenticated proxy servers at managed interfaces.

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation:	FTI must be transmitted securely in a Virtual Desktop Infrastructure (VDI) environment using end-to-end encryption. To use an external web-based system or website that provides FTI over the Internet to a customer, the agency must ensure access to the database through the web application is limited by configuring the system architecture as a three-tier architecture with physically separate systems that provide layered security of the FTI. To access FTI using a web browser, the agency must deploy a web gateway to inspect web traffic and protect the user workstation from direct exposure to the Internet.

Level HIX Implementation Requirements	
Level HIX Implementation:	The information system routes all user-initiated internal communications traffic to untrusted external networks through authenticated proxy servers at managed interfaces.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation:	The information system monitors and controls communications at the external boundary of the system, both physically and logically, and at key internal boundaries within the system. The organization terminates or suspends network connections (i.e., a system-to-system interconnection) upon issuance of an order by the CIO, CISO, or Senior Official for Privacy (SOP). The organization monitors for unauthorized wireless access to information systems and prohibits the installation of wireless access points (WAP) to information systems unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative. If wireless access is authorized, the organization: (i) establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; (ii) authorizes wireless access to the information system prior to allowing such connections; and the organization ensures that (iii) the CMS CIO must approve and distribute the overall wireless plan for his or her respective organization; and (iv) mobile and wireless devices, systems, and networks are not connected to wired HHS/CMS networks except through appropriate controls (e.g., VPN port) or unless specific authorization from HHS/CMS network management has been received.

Control Reference: 01.o Network Routing Control

Control Specification:	Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Network Segmentation; Network Security

Level 1 Implementation Requirements	
Level 1	Applicable to all Organizations

Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation:	Security gateways (e.g., a firewall) are used between internal and external networks (Internet and third-party networks). The organization implements routing controls at the network perimeter.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC6.6 CRR v2016 CM:G2.Q2 CRR v2016 CM:G2.Q8 IRS Pub 1075 v2016 9.4.10 ISO/IEC 27002:2013 13.1.3 ISO/IEC 27799:2016 13.1.3 NIST Cybersecurity Framework v1.1 PR.AC-5 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.PT-4

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 3 Subject to CMMC Level 4 Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to PCI Compliance Subject to State of Massachusetts Data Protection Act Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: Security gateways (e.g., a firewall) are used to validate source and destination addresses at internal and external network control points. The organization designs and implements network perimeters so that all outgoing network traffic to the Internet must pass through at least one application layer filtering proxy server. The proxy supports decrypting network traffic, logging individual TCP sessions, blocking specific URLs,

	domain names, and IP addresses to implement a blacklist, and applying whitelists of allowed sites that can be accessed through the proxy while blocking all other sites. Organizations force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter. The requirements for network routing control are based on the access control policy. Routing controls are also based on positive source and destination address checking mechanisms. Internal directory services and internal IP addresses are protected and hidden from any external access.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CIS CSC v7.1 12.9 CMMC v1.0 SC.3.192-0 CMMC v1.0 SC.4.199-1 CMSRs v3.1 AC-04 (HIGH; MOD) CMSRs v3.1 SC-07 (HIGH; MOD) CRR v2016 CM:G2.Q2 CRR v2016 CM:G2.Q8 FedRAMP AC-4 FedRAMP SC-7 IRS Pub 1075 v2016 9.3.1.4 IRS Pub 1075 v2016 9.3.16.5 IRS Pub 1075 v2016 9.4.10 MARS-E v2 AC-4 MARS-E v2 SC-7 NIST Cybersecurity Framework v1.1 ID.AM-3 NIST Cybersecurity Framework v1.1 PR.AC-5 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.PT-4 NIST SP 800-53 R4 CA-3(2)[S]{0} NIST SP 800-53 R4 CA-3(5)[HM]{0} NIST SP 800-53 R4 SC-30(5)[S]{0} NIST SP 800-53 R4 SC-7(16)[S]{0} NIST SP 800-53 R4 SC-7(9)a[S]{0} NRS 603A.215.1 PCI DSS v3.2.1 1.2 PCI DSS v3.2.1 1.2.1

Level CIS	**Implementation Requirements**
Level CIS Implementation:	The organization disables all workstation-to-workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.

Level CMMC	**Implementation Requirements**
Level CMMC Implementation:	The organization defines and employs tailored network boundary protections in addition to implementing commercially-available solutions.

Level Community Supplemental Reqs 02	**Implementation Requirements**
Level Community Supplemental Reqs 02 Implementation:	The system i) routes Internet traffic through a network intermediary device such as a content-filtering proxy server; ii) prevents end-user systems from communicating directly to the Internet; iii) does not solely rely on host-based controls to route Internet traffic; iv) inspects encrypted Internet traffic; v) uses reputation service to maintain an updated list suspicious domains and URL strings; vi) blocks malicious content, high-risk websites, and uncategorized websites; and vii) analyzes traffic based on more criteria than domain name or IP, including URL, GETs, POSTs, content types (e.g. Flash), and user-agents.

Objective Name: 01.05 Operating System Access Control

Control Objective:	To prevent unauthorized access to operating systems.

Control Reference: 01.p Secure Log-on Procedures

Control Specification:	Access to operating systems shall be controlled by a secure log-on procedure.
Factor Type:	System
Topics:	Authorization; Policies and Procedures; User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to CMMC Level 2 Subject to IRS Pub 1075 Compliance Subject to NIST 800-171 Derived Level Subject to PCI Compliance Subject to Supplemental Requirements
Level 1 Implementation:	A secure log-on procedure: 1. displays a general notice warning that the computer can only be accessed by authorized users; 2. limits the number of unsuccessful log-on attempts allowed to six attempts; 3. enforces recording of unsuccessful and successful attempts; 4. forces a time delay of 30 minutes before further log-on attempts are allowed or reject any further attempts without specific authorization from an administrator; and 5. does not display the password being entered by hiding the password characters with symbols.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) CMMC v1.0 IA.2.082-0 CMSRs v3.1 AC-07 (HIGH; MOD) CMSRs v3.1 AC-08 (HIGH; MOD) CMSRs v3.1 AC-09 (HIGH) CMSRs v3.1 AU-02 (HIGH; MOD) CMSRs v3.1 AU-12 (HIGH; MOD) CMSRs v3.1 IA-06 (HIGH; MOD) FedRAMP AU-12 FedRAMP IA-6 IRS Pub 1075 v2016 9.3.1.7 IRS Pub 1075 v2016 9.3.1.8 IRS Pub 1075 v2016 9.3.3.3 ISO/IEC 27002:2013 9.4.2 ISO/IEC 27799:2016 9.4.2 MARS-E v2 AC-7 MARS-E v2 AU-12 MARS-E v2 AU-2 MARS-E v2 IA-6 NIST 800-171 r2 3.5.11-0 NIST Cybersecurity Framework v1.1 PR.AC-1 NRS 603A.215.1 PCI DSS v3.2.1 8.1.6 PCI DSS v3.2.1 8.1.7 SR v6.4 20.1-0

	SR v6.4 20.3-0 SR v6.4 7a.2-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Does the system(s) transmit or receive data with a third-party? Yes Is the scoped system(s) (on-premise or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? Yes Is the system(s) publicly positioned? Yes Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline
Level 2 Implementation:	Level 1 plus: The procedure for logging into an operating system is designed to minimize the opportunity for unauthorized access. The log-on procedure therefore discloses the minimum of information about the system, in order to avoid providing an unauthorized user with any unnecessary assistance. The log-on procedures: 1. limits the number of unsuccessful log-on attempts allowed to three attempts, and enforces: i. disconnecting data link connections; ii. sending an alarm message to the system console if the maximum number of log-on attempts is reached; and iii. setting the number of password retries in conjunction with the minimum length of the password and the value of the system being protected; 2. limits the maximum and minimum time allowed for the log-on procedure, if exceeded, the system terminates the log-on; 3. does not transmit usernames and passwords in clear text over the network; 4. does not display system or application identifiers until the log-on process has been successfully completed; 5. does not provide help messages during the log-on procedure that would aid an unauthorized user; and 6. validates the log-on information only on completion of all input data. If an error condition arises, the system does not indicate which part of the data is correct or incorrect.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CIS CSC v7.1 16.5 CMSRs v3.1 AC-07 (HIGH; MOD) CMSRs v3.1 IA-06 (HIGH; MOD) FedRAMP IA-6 IRS Pub 1075 v2016 9.3.1.7 IRS Pub 1075 v2016 9.3.7.6 ISO/IEC 27002:2013 9.4.2 ISO/IEC 27799:2016 9.4.2 MARS-E v2 AC-7 MARS-E v2 IA-6 NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST SP 800-53 R4 AC-7[HML]{0} NY DOH SSP v3.1 IA-6[M]-0

Level 3 Implementation Requirements

Level 3	

Organizational Factors:	
Level 3 System Factors:	Is the system(s) accessible from the Internet? Yes
Level 3 Regulatory Factors:	Subject to CMMC Level 2 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: Configure the information system to lock out the user account automatically after three failed log-on attempts by a user during a one-hour time period. Require the lock out to persist for a minimum of three hours. Training includes reporting procedures and responsibility for authorized users to report unauthorized log-ons and unauthorized attempts to log-on. The number of concurrent sessions is limited to a specified number for all account types defined by the organization.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMMC v1.0 AC.2.009-0 CMSRs v3.1 AC-07 (HIGH; MOD) CMSRs v3.1 AC-10 (HIGH) CMSRs v3.1 AT-02 (HIGH; MOD) FedRAMP AC-7 FedRAMP AT-2 HITRUST IRS Pub 1075 v2016 9.3.1.7 ISO/IEC 27002:2013 7.2.2 ISO/IEC 27002:2013 9.4.2 ISO/IEC 27799:2016 7.2.2 ISO/IEC 27799:2016 9.4.2 MARS-E v2 AC-10 MARS-E v2 AC-7 MARS-E v2 AC-9 MARS-E v2 AT-2 NIST 800-171 r2 3.1.8-0 NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.AT-1 NIST Cybersecurity Framework v1.1 PR.DS-5 NY DOH SSP v3.1 AC-7.IS1[M]-2 NY DOH SSP v3.1 AC-7a[M]-0

Level CMS Implementation Requirements

Level CMS Implementation:	The number of concurrent network sessions for a user is limited and enforced to one session. The number of concurrent application/process sessions is limited and enforced to the number of sessions expressly required for the performance of job duties. The requirement and use of more than one application/process session for each user are documented in the system security profile. The organization configures the information system to lock out the user account automatically after 3 invalid login attempts during a 120-minute time window and requires the lock out to persist until released by an administrator.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The number of concurrent network sessions for a user is limited and enforced to three sessions for privileged access and two sessions for non-privileged access.

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation:	Automatically lock the account/node until an authorized system administrator reinstates the account.

Control Reference: 01.q User Identification and Authentication

Control Specification:	All users shall have a unique identifier (user ID) for their personal use only, and an authentication technique shall be implemented to substantiate the claimed identity of a user. *Required for HITRUST Certification CSF v9.6
Factor Type:	System
Topics:	Authentication; User Access

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to CMMC Level 1 Subject to CMMC Level 2 Subject to CMMC Level 3 Subject to HIPAA Security Rule Subject to HITRUST De-ID Framework Requirements Subject to NIST 800-171 Basic Level Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to State of Massachusetts Data Protection Act Subject to Supplemental Requirements Subject to Texas Health and Safety Code
Level 1 Implementation:	Before allowing access to system components or data, the organization requires verifiable unique IDs for all types of users including, but not limited to: 1. technical support personnel; 2. operators; 3. network administrators; 4. system programmers; and 5. database administrators. The following is required for each category of User ID: 1. regular User IDs: i. user IDs are used to trace activities to the responsible individual; and

	ii. regular user activities are not performed from privileged accounts. 2. shared user/group IDs: i. in exceptional circumstances, where there is a clear business benefit, the use of a shared user ID for a group of users or a specific job can be used; ii. approval by management is documented for such cases; and iii. additional controls are required to maintain accountability. 3. generic IDs: i. generic IDs for use by an individual are only allowed either where the functions accessible or actions carried out by the ID do not need to be traced (e.g., read-only access). The organization ensures that redundant user IDs are not issued to other users. Non-organizational users, or processes acting on behalf of non-organizational users, determined to need access to information residing on the organization's information systems, are uniquely identified, and authenticated. Users are uniquely identified and authenticated for both local and remote accesses to information systems using a username and password (see 01.d) at a minimum or preferably a username and password supplemented or replaced by risk-based (non-static) and/or strong authentication methods. Access to PMI data and any other data deemed extremely sensitive (e.g., by statute) is considered privileged and requires multi-factor authentication. The requirement for risk-based, strong, and multi-factor authentication methods is determined by the organization's risk assessment and its application commensurate with the type of data, level of sensitivity of the information, and user type. Electronic signatures, unique to one individual, ensures that the signature cannot be reused by, or reassigned to, anyone else.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 201 CMR 17.04(1)(a) 201 CMR 17.04(2)(b) 21 CFR Part 11.10(d) 21 CFR Part 11.10(g) 21 CFR Part 11.100(a) 45 CFR Part § 164.312(a)(2)(i) HIPAA.SR-0 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 1 153: Eligibility and Benefits Connectivity Rule v1.1.0 Subsection 5.2 CMMC v1.0 AU.2.041-0 CMMC v1.0 IA.1.076-1 CMMC v1.0 IA.1.077-1 CMMC v1.0 IA.3.085-0 CMMC v1.0 SC.3.182-2 CMSRs v3.1 AC-06(02) (HIGH; MOD) CMSRs v3.1 CM-08(03) (HIGH; MOD) CMSRs v3.1 IA-02 (HIGH; MOD) CMSRs v3.1 IA-04 (HIGH; MOD) CMSRs v3.1 IA-08 (HIGH; MOD) COBIT 5 DS5.3 COBIT 5 DSS05.04 CRR v2016 CCM:G2.Q4 CSA CCM v3.0.1 IAM-04 De-ID Framework v1 Identification and Authentication (System-level): Authentication Policy De-ID Framework v1 Identification and Authentication: Authentication Policy FedRAMP AC-6(2) FedRAMP IA-2 FedRAMP IA-3 FedRAMP IA-4 FedRAMP IA-8 IRS Pub 1075 v2016 9.3.7.2 IRS Pub 1075 v2016 9.3.7.4 IRS Pub 1075 v2016 9.3.7.8 ISO/IEC 27002:2013 9.2.1 ISO/IEC 27002:2013 9.2.3

	ISO/IEC 27799:2016 9.2.1 ISO/IEC 27799:2016 9.2.3 MARS-E v2 AC-6(2) MARS-E v2 IA-2 MARS-E v2 IA-4 MARS-E v2 IA-8 NIST 800-171 r2 3.13.4-2 NIST 800-171 r2 3.3.2-0 NIST 800-171 r2 3.5.1-1 NIST 800-171 r2 3.5.2-1 NIST 800-171 r2 3.5.5-0 NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.AT-2 NIST SP 800-53 R4 IA-2[HML]{0} NIST SP 800-53 R4 IA-4(1)[S]{0} NIST SP 800-53 R4 IA-8[HML]{0} NRS 603A.215.1 NY DOH SSP v3.1 AC-17.IS4d[M]-2 NY DOH SSP v3.1 AC-2(9).NYS[MN]-1 NY DOH SSP v3.1 AC-2(9).NYS3[MN]-0 NY DOH SSP v3.1 AC-2(9)[MN]-0 NY DOH SSP v3.1 IA-2.IS1[M]-2 NY DOH SSP v3.1 IA-2[M]-0 NY DOH SSP v3.1 IA-8[M]-0 NY DOH SSP v3.1 MA-4b[M]-2 PCI DSS v3.2.1 12.3.2 PCI DSS v3.2.1 8.1 PCI DSS v3.2.1 8.1.1 PCI DSS v3.2.1 8.5 PMI DSP Framework PR.AC-1 PMI DSP Framework PR.AC-2 PMI DSP Framework PR.AC-3 SR v6.4 18.1-0 SR v6.4 7b.3-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Is the scoped system(s) (on-premise or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? Yes Is the system(s) accessible from the Internet? Yes
Level 2 Regulatory Factors:	Subject to 23 NYCRR 500 Subject to FISMA Compliance Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: Appropriate authentication methods including strong authentication methods in addition to passwords are used for communicating through an external, non-organization-controlled network (e.g., the Internet). Help desk support requires user identification for any transaction that has information security implications. During the registration process to provide new or replacement hardware tokens, in-person verification is required in front of a designated registration authority with authorization by a designated organizational official (e.g., a supervisor). When PKI-based authentication is used, the information system:

	1. validates certificates by constructing a certification path with status information to an accepted trust anchor; 2. validates certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; 3. enforces authorized access to the corresponding private key; 4. maps the authenticated identity to the account of the individual or group; and 5. implements a local cache of revocation data to support path discovery and validation in case of an inability to access revocation information via the network. The information system uses replay-resistant authentication mechanisms such as nonce, one-time passwords, or timestamps to secure network access for privileged accounts. The organization requires that access for all accounts, including those for network and security devices, is to be obtained through a centralized point of authentication, for example Active Directory or LDAP. Electronic signatures based upon biometrics are designed to ensure that they cannot be used by any individual other than their genuine owners. Electronic signatures and handwritten signatures executed to electronic records are linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means. Signed electronic records contain information associated with the signing that clearly indicates the following in human-readable format: 1. Printed name of the signer 2. The date and time when the signature was executed; and 3. The meaning of the signature (e.g., review, approval, responsibility, authorship)
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.200(b) 21 CFR Part 11.50(a) 21 CFR Part 11.50(b) 21 CFR Part 11.70 CIS CSC v7.1 11.5 CIS CSC v7.1 4.5 CMSRs v3.1 IA-02 (HIGH; MOD) CMSRs v3.1 IA-02(08) (HIGH; MOD) CMSRs v3.1 IA-02(11) (HIGH; MOD) CMSRs v3.1 IA-05(02) (HIGH; MOD) CMSRs v3.1 IA-05(03) (HIGH; MOD) CMSRs v3.1 IA-05(11) (HIGH; MOD) FedRAMP IA-2 FedRAMP IA-2(8) FedRAMP IA-5 FedRAMP IA-5(11) FedRAMP IA-5(2) FedRAMP IA-5(3) IRS Pub 1075 v2016 9.3.7.2 IRS Pub 1075 v2016 9.3.7.5 ISO/IEC 27002:2013 9.2.1 ISO/IEC 27799:2016 9.2.1 MARS-E v2 IA-2 MARS-E v2 IA-2(8) MARS-E v2 IA-5(2) MARS-E v2 IA-5(3) NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.AC-3 NIST Cybersecurity Framework v1.1 PR.MA-2 NIST SP 800-53 R4 AC-24(2)[S]{0} NIST SP 800-53 R4 AU-10(1)a[S]{2} NIST SP 800-53 R4 AU-10(2)[S]{2} NIST SP 800-53 R4 AU-10(4)[S]{2} NIST SP 800-53 R4 IA-10[S]{0}

	NIST SP 800-53 R4 IA-2(8)[HM]{0} NIST SP 800-53 R4 IA-5(12)[S]{0} NIST SP 800-53 R4 IA-5(13)[S]{1} NIST SP 800-53 R4 IA-5(14)[S]{0} NIST SP 800-53 R4 IA-5(2)[HM]{0} NIST SP 800-53 R4 SC-11(1)[S]{0} NIST SP 800-53 R4 SC-11[S]{0} NIST SP 800-53 R4 SC-7(15)[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 IA-2(11)[M]-1 NY DOH SSP v3.1 IA-2(8)[M]-0 NY DOH SSP v3.1 IA-2.IS2[M]-0 NY DOH SSP v3.1 IA-5(2)a[M]-0 NY DOH SSP v3.1 IA-5(2)b[M]-0 NY DOH SSP v3.1 IA-5(2)c[M]-0 NY DOH SSP v3.1 IA-5(2)d[M]-0 PCI DSS v3.2.1 8.2.2 PCI DSS v3.2.1 8.3.2 PCI DSS v3.2.1 8.5.1 PCI DSS v3.2.1 8.6

Level 3 Implementation Requirements

Level 3 Organizational Factors:	
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 2 Subject to CMMC Level 3 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Supplemental Requirements Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: The organization employs multifactor authentication for remote network access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access. The organization employs multifactor authentication for local access to privileged accounts (including those used for non-local maintenance and diagnostic sessions).
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CIS CSC v7.1 4.5 CMMC v1.0 IA.3.083-0 CMMC v1.0 MA.2.113-1 CMSRs v3.1 IA-02(01) (HIGH; MOD) CMSRs v3.1 IA-02(02) (HIGH; MOD) CMSRs v3.1 IA-02(03) (HIGH; MOD) CMSRs v3.1 IA-02(04) (HIGH) CMSRs v3.1 IA-02(11) (HIGH) CMSRs v3.1 IA-02(12) (HIGH; MOD) FedRAMP IA-2(1) FedRAMP IA-2(11) FedRAMP IA-2(12) FedRAMP IA-2(2) FedRAMP IA-2(3)

	IRS Pub 1075 v2016 9.3.7.2 IRS Pub 1075 v2016 Exhibit 10 MARS-E v2 IA-2(1) MARS-E v2 IA-2(11) MARS-E v2 IA-2(2) MARS-E v2 IA-2(3) NIST 800-171 r2 3.5.3-0 NIST 800-171 r2 3.7.5-1 NIST SP 800-53 R4 IA-2(1)[HML]{0} NIST SP 800-53 R4 IA-2(11)[HM]{1} NIST SP 800-53 R4 IA-2(2)[HM]{0} NIST SP 800-53 R4 IA-2(3)[HM]{0} NIST SP 800-53 R4 IA-2(6)[S]{1} NIST SP 800-53 R4 IA-2(7)[S]{1} NIST SP 800-53 R4 MA-4c[HML]{2} NY DOH SSP v3.1 IA-2(1)[M]-0 NY DOH SSP v3.1 IA-2(11)[M]-2 NY DOH SSP v3.1 IA-2(2)[M]-0 NY DOH SSP v3.1 IA-2(3)[M]-0 NY DOH SSP v3.1 IA-2(6)[MN]-0 NY DOH SSP v3.1 IA-2(7)[MN]-0 NY DOH SSP v3.1 MA-4b[M]-1 SR v6.4 40-0 SR v6.4 49-0

Level CIS	Implementation Requirements
Level CIS Implementation:	The organization requires access for all accounts, including those for network and security devices, to be obtained through a centralized point of authentication, for example Active Directory or LDAP. Ensure that all accounts have an expiration date that is monitored and enforced.

Level CMS	Implementation Requirements
Level CMS Implementation:	The information system uses multifactor authentication for local access to non-privileged accounts. The information system uses replay-resistant authentication mechanisms such as nonce, one-time passwords, or time stamps (e.g., Kerberos, TLS, etc.) for network access to non-privileged accounts. A risk assessment is used in determining the authentication needs of the organization. The information system, for hardware token-based authentication, employs mechanisms that satisfy minimum token requirements discussed in the Risk Management Handbook (RMH), Volume III, Standard 3.1, CMS Authentication Standards.

Level Community Supplemental Reqs 02	Implementation Requirements
Level Community Supplemental Reqs 02 Implementation:	The organization requires the use of multifactor authentication for privileged access to administrative network zones. The organization manages access to all shared privileged accounts such that individual accountability are preserved, and credentials are not synchronized across environments.

Level FedRAMP	Implementation Requirements
Level FedRAMP Implementation:	The organization requires individuals to be authenticated with an individual authenticator as a second level of authentication when a group authenticator is employed.

	The organization manages individual identifiers, such as on personnel badges or email, by uniquely identifying each individual as an employee, contractor, volunteer, student or other such organization-defined classification.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	Complete section 2.10 (e-Authentication level) in the SSP Template. Two-factor authentication is required whenever FTI is being accessed from an alternative work location or if accessing FTI via an agency's web portal by an employee or contractor. The agency configures the web services to be authenticated before access is granted to users via an authentication server. All web portal and two-factor authentication requirements apply in a data warehouse environment. Authentication is required both at the operating system level and at the application level, whenever the data warehousing environment is accessed.

Level HIX Implementation Requirements

Level HIX Implementation:	The information system, for hardware token-based authentication, employs organization-specified mechanisms that satisfy generally acceptable minimum token requirements.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The information system implements organization-defined out-of-band authentication under organization-defined conditions. The organization ensures email cannot be used to transmit the random authenticator for the Out-of-Band (OOB) token. The organization manages information system identifiers by: (i) receiving authorization from defined personnel or roles (defined in the applicable security plan) to assign an individual, group, role, or device identifier; (ii) selecting an identifier that identifies an individual, group, role, or device; (iii) assigning the identifier to the intended individual, group, role, or device; (iv) preventing reuse of identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of three [3] years or more has passed; and (v) disabling the identifier after sixty [60] days of inactivity for Moderate systems. The organization ensures social security numbers (SSNs), and parts of SSNs, are not used as system identifiers. Identifier management ensures that any access to, or action involving, personally identifiable information (PII) is attributable to a unique individual. The organization manages information system authenticators by (i) verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; (ii) establishing initial authenticator content for authenticators defined by the organization; (iii) ensuring that authenticators have sufficient strength of mechanism for their intended use; (iv) establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; (v) changing default content of authenticators prior to information system installation; (vi) establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; (vii) changing/refreshing authenticators as follows: (a) passwords are valid for no longer than the period directed in IA-5 (1) immediately in the event of known or suspected compromise, and immediately upon system installation (e.g. default or vendor-supplied

	passwords); (b) PIV compliant access cards are valid for no longer than five [5] years; (c) PKI certificates issued in accordance with the Federal PKI Common Policy are valid for no longer than three [3] years; and (d) any PKI authentication request must be validated by Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) to ensure that the certificate being used for authentication has not been revoked. (viii) Protecting authenticator content from unauthorized disclosure and modification; (ix) requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and (x) changing authenticators for group/role accounts when membership to those accounts' changes. The organization creates, enables, modifies, disables, and removes information system accounts in accordance with Acceptable Risk Safeguards (ARS) requirements and Risk Management Handbook (RMH) Standards and Procedures. The organization only permits the use of shared/group accounts that meet the requirement to uniquely attribute user activity to an account. The organization documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication. Multifactor authentication (MFA) is required before being granted access to CMS email. Multifactor authentication (MFA) access control mechanisms must meet CMS approved standards discussed in the RMH, Volume III, Standard 3.1, CMS Authentication Standards.

Level PCI	Implementation Requirements
Level PCI Implementation:	The organization does not use group, shared, or generic IDs, passwords, or other authentication methods as follows: 1. generic user IDs are disabled or removed. 2. shared user IDs do not exist for system administration and other critical functions. 3. shared and generic user IDs are not used to administer any system components. Where other authentication mechanisms are used (e.g., physical, or logical security tokens, smart cards, and certificates), use of these mechanisms is assigned as follows: 1. authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. 2. Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access. Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase for each customer).

Level Supplemental Requirements	Implementation Requirements
Level Supplemental Requirements Implementation:	Maintain individual ownership and accountability for use of all service accounts.

Control Reference: 01.r Password Management System

Control Specification:	Systems for managing passwords shall be interactive and shall ensure quality passwords.
Factor Type:	System
Topics:	Cryptography; Password Management

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to HIPAA Security Rule Subject to Supplemental Requirements Subject to Texas Health and Safety Code
Level 1 Implementation:	Refer to Sections 1.b and 1.f for a full list of password controls. In addition, a password management system is implemented to: 1. require the use of individual user IDs and passwords to maintain accountability; 2. allow users to select and change their own passwords and include a confirmation procedure to allow for input errors; 3. force users to change temporary passwords at the first log-on (see 01.b); 4. not display passwords on the screen when being entered; and 5. always change vendor-supplied defaults before installing a system on the network including passwords, simple network management protocol (SNMP) community strings and the elimination of unnecessary accounts.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 201 CMR 17.04(1)(b) 45 CFR Part § 164.308(a)(5)(ii)(D) HIPAA.SR-1 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 1 153: Eligibility and Benefits Connectivity Rule v1.1.0 Subsection 5.2 CMSRs v3.1 IA-05 (HIGH; MOD) FedRAMP IA-5 IRS Pub 1075 v2016 9.3.7.5 ISO/IEC 27002:2013 9.2.4 ISO/IEC 27002:2013 9.4.3 ISO/IEC 27799:2016 9.2.4 ISO/IEC 27799:2016 9.4.3 MARS-E v2 IA-5 NIST Cybersecurity Framework v1.1 PR.AC-1 NRS 603A.215.1 PCI DSS v3.2.1 2.1 SR v6.4 6.4-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Does the system(s) transmit or receive data with a third-party? Yes Is the scoped system(s) (on-premise or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? Yes Is the system(s) accessible from the Internet? Yes Is the system(s) publicly positioned? Yes Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	Subject to FedRAMP Certification Subject to FISMA Compliance Subject to HIPAA Security Rule

	Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to PCI Compliance Subject to State of Massachusetts Data Protection Act Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: Refer to Sections 1.b and 1.f for a full list of password controls. The password management system: 1. stores and transmits passwords in protected (e.g., encrypted or hashed) form; 2. stores password files separately from application system data; 3. enforces a choice of quality passwords (see 01.b); 4. enforces password changes (see 01.b); and 5. maintains a record of previous user passwords and prevents re-use (see 01.b).
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 201 CMR 17.04(1)(c) 45 CFR Part § 164.308(a)(5)(ii)(D) HIPAA.SR-2 CMSRs v3.1 IA-05 (HIGH; MOD) CMSRs v3.1 IA-05(01) (HIGH; MOD) FedRAMP IA-5 IRS Pub 1075 v2016 9.3.7.5 ISO/IEC 27002:2013 9.4.3 ISO/IEC 27799:2016 9.4.3 MARS-E v2 IA-5 MARS-E v2 IA-5(1) NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.DS-2 NIST Cybersecurity Framework v1.1 PR.DS-5 NRS 603A.215.1 PCI DSS v3.2.1 8.2.1

Level CMS Implementation Requirements

Level CMS Implementation:	The CMS information system for PKI-based authentication: 1. validates certificates by constructing a certification path with status information to an accepted trust anchor; 2. enforces authorized access to the corresponding private key; and 3. maps the authenticated identity to the user account.

Control Reference: 01.s Use of System Utilities

Control Specification:	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
Factor Type:	System
Topics:	Authorization; Monitoring; Network Segmentation

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Supplemental)

Level 1 Implementation:	The use of system utilities (e.g., administrative tools in Windows, the settings section--specifically network/device/security configuration--on VoIP phones, etc.) is controlled by implementing the following: 1. use of identification, authentication, and authorization procedures for system utilities; 2. segregation of system utilities from applications software; and 3. limitation of the use of system utilities to the minimum practical number of trusted, authorized users (see CSF control 01.b thru 01.o).
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC6.1 AICPA 2017 CC6.2 CMSRs v3.1 AC-06 (HIGH; MOD) CSA CCM v3.0.1 IAM-13 FedRAMP AC-6 FFIEC IS v2016 A.6.21(a) IRS Pub 1075 v2016 9.3.1.6 ISO/IEC 27002:2013 9.4.4 ISO/IEC 27799:2016 9.4.4 MARS-E v2 AC-6 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.PT-3 NIST SP 800-53 R4 MA-3(4)[S]{0} NIST SP 800-53 R4 SI-10(1)b[S]{0}

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Does the system(s) transmit or receive data with a third-party? Yes Is the scoped system(s) (on-premise or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? Yes Is the system(s) accessible from the Internet? Yes Is the system(s) publicly positioned? Yes Number of interfaces to other systems 25 to 75
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to Supplemental Requirements Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The use of system utilities is controlled by implementing the following: 1. authorization for ad hoc use of systems utilities; 2. limitation of the availability of system utilities (e.g., limitation of availability by setting restrictive file system-level permissions for the access and execution of system utilities such as cmd.exe, ping, tracert, ipconfig, ifconfig, etc.); 3. disabling public "read" access to files, objects, and directories; 4. logging of all use of system utilities; 5. defining and documenting authorization levels for system utilities; 6. deletion of, or file system file execution permission denial of, all unnecessary software-based utilities and system software; and

	7. not making system utilities available to users who have access to applications on systems where segregation of duties is required. The information system owner regularly reviews the system utilities available to identify and eliminate unnecessary functions, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. Public "read" and "write" access to all system files, objects, and directories are disabled.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 AC-03 (HIGH; MOD) COBIT 5 DS5.7 COBIT 5 DSS05.05 FedRAMP AC-3 FFIEC IS v2016 A.6.21(a) IRS Pub 1075 v2016 9.3.1.3 ISO/IEC 27002:2013 9.4.4 ISO/IEC 27799:2016 9.4.4 MARS-E v2 AC-3 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.PT-3 NRS 603A.215.1 NY DOH SSP v3.1 AC-3.IS2[M]-0 PCI DSS v3.2.1 2.2.5 SR v6.4 6.3-2

Control Reference: 01.t Session Time-out

Control Specification:	Inactive sessions shall shut down after a defined period of inactivity. *Required for HITRUST Certification CSF v9.6
Factor Type:	System
Topics:	User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 2 Subject to CMMC Level 3 Subject to FISMA Compliance Subject to HIPAA Security Rule Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to Texas Health and Safety Code
Level 1 Implementation:	A time-out system that conceals information previously visible on the display with a publicly viewable image (e.g., a screen saver) pauses the session screen after 15 minutes of inactivity and closes network sessions after 30 minutes of inactivity. The system requires the user to reestablish access using appropriate identification and authentication procedures. A limited form of time-out system can be provided for legacy systems that cannot be modified to accommodate this requirement, which clears the screen and prevents

	unauthorized access through re-authentication requirements to continue the active session but does not close down the application or network sessions.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(d) 45 CFR Part § 164.312(a)(2)(iii) HIPAA.SR-0 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CIS CSC v7.1 16.11 CMMC v1.0 AC.2.010-0 CMMC v1.0 SC.3.186-0 CMSRs v3.1 AC-11 (HIGH; MOD) CMSRs v3.1 AC-11(01) (HIGH; MOD) CSA CCM v3.0.1 AIS-04 CSA CCM v3.0.1 MOS-14 FedRAMP AC-11 FedRAMP AC-11(1) FedRAMP AC-12 IRS Pub 1075 v2016 9.3.1.10 IRS Pub 1075 v2016 9.3.1.9 ISO/IEC 27002:2013 9.4.2 ISO/IEC 27799:2016 9.4.2 MARS-E v2 AC-11 MARS-E v2 AC-11(1) MARS-E v2 AC-12 NIST 800-171 r2 3.1.10-0 NIST 800-171 r2 3.13.9-0 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.PT-4 NIST SP 800-53 R4 AC-11[HM]{0} NRS 603A.215.1 NY DOH SSP v3.1 AC-11.IS1[M]-0 NY DOH SSP v3.1 AC-11a[M]-1 NY DOH SSP v3.1 AC-11b[M]-0 NY DOH SSP v3.1 AC-2(5).NYS1[HN]-2 NY DOH SSP v3.1 AC-2(5).NYS3[HN]-0 PCI DSS v3.2.1 12.3.8 PCI DSS v3.2.1 8.1.8

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Is the system(s) publicly positioned? Yes
Level 2 Regulatory Factors:	Subject to FedRAMP Certification Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: For systems that are publicly positioned, a time-out system (e.g., a screen saver) pauses the session screen after 2 minutes of inactivity and closes network sessions after 30 minutes of inactivity.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CIS CSC v7.1 16.11 CMSRs v3.1 AC-11 (HIGH; MOD) CMSRs v3.1 AC-11(01) (HIGH; MOD) CMSRs v3.1 AC-12 (HIGH; MOD) CMSRs v3.1 SC-10 (HIGH; MOD) FedRAMP AC-12 FedRAMP AC-2(5) FedRAMP SC-10 IRS Pub 1075 v2016 9.3.1.10 IRS Pub 1075 v2016 9.3.1.9

	IRS Pub 1075 v2016 9.3.16.7 ISO/IEC 27002:2013 9.4.2 ISO/IEC 27799:2016 9.4.2 MARS-E v2 AC-11 MARS-E v2 AC-11(1) MARS-E v2 SC-10 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.PT-4 NRS 603A.215.1 PCI DSS v3.2.1 12.3.8 PCI DSS v3.2.1 8.1.8
Level CMS Implementation Requirements	
Level CMS Implementation:	The organization requires that users log out when the time-period of expected inactivity exceeds 90 minutes and at the end of the user's normal work period. The information system automatically terminates the network connection at the end of the session; otherwise, the system forcibly (i) disconnects VPN connections after 30 minutes or less of inactivity; and (ii) de-allocates DHCP leases after 7 days consecutive days of network connectivity.
Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation:	The organization forcibly disconnects inactive VPN connections after 15 minutes of inactivity. The information system must automatically terminate a user session after 15 minutes of inactivity.
Level HIX Implementation Requirements	
Level HIX Implementation:	The information system automatically terminates the network connection associated with a communications session at the end of the session, or: 1. Forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven days; and 2. Forcibly disconnects inactive Virtual Private Network (VPN) connections after 30 minutes of inactivity.
Level NYDOH Implementation Requirements	
Level NYDOH Implementation:	Remote access sessions must not last any longer than twenty-four [24] hours. The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image. The information system automatically terminates a user session after defined conditions or trigger events (defined in the applicable security plan) requiring session disconnect. The information system terminates or suspends network connections (i.e., a system-to-system interconnection) upon issuance of an order by the CMS CIO, CISO, or Senior Official for Privacy (SOP).
Level Supplemental Requirements	**Implementation Requirements**

Level Supplemental Requirements Implementation:	A time-out mechanism (e.g., screensaver) pauses the session screen after 15 minutes of inactivity, closes network sessions after 30 minutes of inactivity, and requires the user to reestablish authenticated access once the session has been paused or closed.

Control Reference: 01.u Limitation of Connection Time

Control Specification:	Restrictions on connection times shall be used to provide additional security for high-risk applications.
Factor Type:	System
Topics:	Authentication; Authorization; User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	
Level 1 Implementation:	Connection time controls are implemented for sensitive computer applications, especially from high-risk locations (e.g., public, or external areas that are outside the organization's security management) including: 1. using predetermined time slots (e.g., for batch file transmissions or regular interactive sessions of short duration); 2. restricting connection times to normal office hours if there is no requirement for overtime or extended-hours operation; and 3. re-authentication at timed intervals.
Level 1 Control Standard Mapping:	21 CFR Part 11.10(d) FFIEC IS v2016 A.6.22(e) ISO/IEC 27002:2013 9.4.2 ISO/IEC 27799:2016 9.4.2 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.PT-3 NIST Cybersecurity Framework v1.1 PR.PT-4

Objective Name: 01.06 Application and Information Access Control

Control Objective:	To prevent unauthorized access to information held in application systems.

Control Reference: 01.v Information Access Restriction

Control Specification:	Logical and physical access to information and application systems and functions by users and support personnel shall be restricted in accordance with the defined access control policy. *Required for HITRUST Certification CSF v9.6
Factor Type:	System
Topics:	Authentication; Policies and Procedures; User Access; Viruses and Malware

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Supplemental) Subject to Texas Health and Safety Code
Level 1 Implementation:	Restrictions to access are based on individual business application requirements and in accordance with the access control policy. Access rights to applications and application functions should be restricted in accordance with the access control policy. Associated identification and authentication controls are developed, disseminated, and periodically reviewed and updated, including: 1. specific user actions that can be performed on the information system without identification or authentication are identified and supporting rationale documented; 2. actions to be performed without identification and authentication are permitted only to the extent necessary to accomplish mission objectives;
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 AC-06 (HIGH; MOD) CRR v2016 CCM:G2.Q4 CSA CCM v3.0.1 IAM-09 FedRAMP AC-6 FFIEC IS v2016 A.6.22(b) FFIEC IS v2016 A.6.27(b) FFIEC IS v2016 A.6.8(a) FFIEC IS v2016 A.6.8(c) FFIEC IS v2016 A.8.1(k) IRS Pub 1075 v2016 9.3.1.6 ISO/IEC 27002:2013 9.4.1 ISO/IEC 27799:2016 9.4.1 MARS-E v2 AC-6 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.PT-3 NIST SP 800-53 R4 AC-25[S]{0} NIST SP 800-53 R4 AC-3(3)[S]{2}

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to CRR V2016 Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline

	Subject to the CMS Minimum Security Requirements (High) Subject to the EU GDPR
Level 2 Implementation:	Level 1 plus: The following guidelines are implemented in order to support access restriction requirements: 1. controlling access rights to other applications according to applicable access control policies; 2. ensuring that outputs from application systems handling covered information contain only the information relevant to the use of the output and are sent only to authorized terminals and locations; and 3. performing periodic reviews of such outputs to ensure that redundant information is removed. When encryption of stored information is employed as an access enforcement mechanism, it is encrypted using validated cryptographic modules (see 06.d). Data stored in the information system is protected with system access controls including file system, network share, claims, application, and/or database specific access control lists and is encrypted when residing in non-secure areas. Specific user actions that can be performed on the information system without identification or authentication are identified and supporting rationale documented. Actions to be performed without identification and authentication are permitted only to the extent necessary to accomplish mission objectives.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CIS CSC v7.1 14.6 CMSRs v3.1 AC-03 (HIGH; MOD) CMSRs v3.1 AC-14 (HIGH; MOD) CMSRs v3.1 DM-01 (HIGH; MOD) CMSRs v3.1 SC-15 (HIGH; MOD) CRR v2016 CM:G2.Q3 FedRAMP AC-4 FedRAMP SC-15 FFIEC IS v2016 A.8.1(k) IRS Pub 1075 v2016 4.7.2 IRS Pub 1075 v2016 9.3.1.11 IRS Pub 1075 v2016 9.3.1.3 IRS Pub 1075 v2016 9.3.1.4 IRS Pub 1075 v2016 9.3.16.10 IRS Pub 1075 v2016 Exhibit 10 ISO/IEC 27002:2013 9.4.1 ISO/IEC 27799:2016 9.4.1 MARS-E v2 AC-14 MARS-E v2 AC-3 MARS-E v2 DM-1 MARS-E v2 SC-15 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.AC-7 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.PT-3 NIST SP 800-53 R4 AC-14a[HML]{0} NY DOH SSP v3.1 AC-14a[M]-0 NY DOH SSP v3.1 AC-14c[M]-0

Level 3 Implementation Requirements

Level 3 Organizational Factors:	
Level 3 System Factors:	Is the scoped system(s) (on-premise or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? Yes Is the system(s) accessible from the Internet? Yes

Level 3 Regulatory Factors:	Subject to Banking Requirements Subject to FedRAMP Certification Subject to PCI Compliance
Level 3 Implementation:	Level 2 plus: For individuals accessing sensitive information (e.g., covered information, cardholder data) from a remote location, prohibit the copy, move, print (and print screen) and storage of this information onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. The organization restricts the use of database management utilities to only authorized database administrators. Users are prevented from accessing database data files at the logical data view, field, or field-value levels. Column-level access controls are implemented to restrict database access.
Level 3 Control Standard Mapping:	NIST Cybersecurity Framework v1.1 PR.AC-3 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.PT-2 NIST Cybersecurity Framework v1.1 PR.PT-3 NRS 603A.215.1 PCI DSS v3.2.1 12.3.10

Level CMS Implementation Requirements

Level CMS Implementation:	Encryption as access enforcement extends to all government and non-government furnished desktop computers that store sensitive information. While encryption is the preferred technical solution for protection of sensitive information on all desktop computers, adequate physical security controls and other management controls are acceptable mitigations for the protection of desktop computers with the approval of the CIO or his/her designated representative. If encryption is used as an access control mechanism it must meet CMS approved (FIPS 140-2 compliant and a NIST validated module) encryption standards.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	Access to FTI must be explicitly authorized strictly on a need-to-know basis. FTI must never be indiscriminately disseminated, even within the recipient agency, body, or commission. No person is given more FTI than is needed for performance of his/her duties. Document and provide supporting rationale in the SSR for the information system the user actions not requiring identification or authentication. The organization ensures that only authorized users with a demonstrated need-to-know can query FTI data within a data warehouse. To use a virtual environment that receives, processes, stores, or transmits FTI, the agency must restrict access to FTI to authorized users when FTI is stored in a shared location.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	Data stored in the information system must be protected with system access controls and must be encrypted when residing in non-secure areas. If wireless access is explicitly approved, wireless device service set identifier broadcasting is disabled and the following wireless restrictions and access controls are implemented: (i) encryption protection is enabled; (ii) access points are placed in secure areas; (iii) access points are shut down when not in use (i.e., nights, weekends); (iv) a stateful inspection firewall is implemented between the wireless network and the wired infrastructure; (v) MAC address authentication is utilized; (vi) static IP addresses, not Dynamic Host Configuration Protocol (DHCP), is utilized; (vii) personal firewalls are utilized on all wireless clients; (viii) file sharing is disabled on all wireless clients; (ix) intrusion detection agents are deployed on the wireless side of the firewall; (x) wireless activity is monitored and recorded, and the records are reviewed on a regular basis; (xi) adheres to CMS-CIO-POL-INF12-01, CMS Policy for Wireless Client Access; and (xii) adheres to the HHS Standard for IEEE 802.11 Wireless Local Area Network (WLAN), and (xiii) wireless printers and all Bluetooth devices such as keyboards are not allowed. The organization prohibits the use of external information systems, including but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports to store, access, transmit, or process sensitive information, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If external information systems are authorized to store, access, transmit, or process sensitive information, the organization establishes strict terms and conditions for their use. The terms and conditions must address, at a minimum: (i) the types of applications that can be accessed from external information systems; (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted; (iii) how other users of the external information system will be prevented from accessing federal information; (iv) the use of VPN and stateful inspection firewall technologies; (v) the use of and protection against the vulnerabilities of wireless technologies; (vi) the maintenance of adequate physical security controls; (vii) the use of virus and spyware protection software; and (viii) how often the security capabilities of installed software are to be updated.

Level PCI Implementation Requirements

Level PCI Implementation:	Where there is an authorized business need to allow the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media for personnel accessing cardholder data via remote-access technologies, the organizations usage policies requires the data to be protected in accordance with all applicable PCI DSS requirements. All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: 1. all user access to, user queries of, and user actions on databases are through programmatic methods. 2. only database administrators have the ability to directly access or query databases. Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).

Control Reference: 01.w Sensitive System Isolation

Control Specification:	Sensitive systems shall have a dedicated and isolated computing environment. *Required for HITRUST Certification CSF v9.6
Factor Type:	System
Topics:	IT Organization and Management Roles and Responsibilities; Network Segmentation; Network Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Supplemental)
Level 1 Implementation:	The sensitivity of an application system is explicitly identified and documented by the application owner.
Level 1 Control Standard Mapping:	CMSRs v3.1 RA-02 (HIGH; MOD) FedRAMP RA-2 MARS-E v2 RA-2 NIST Cybersecurity Framework v1.1 ID.AM-5 NIST Cybersecurity Framework v1.1 ID.BE-3 NIST SP 800-53 R4 AC-16b[S]{1}

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	Subject to CMMC Level 4 Subject to CRR V2016 Subject to Supplemental Requirements
Level 2 Implementation:	Level 1 plus: The sensitive application system runs on a dedicated computer, or only share resources with trusted applications systems. Isolation is achieved using physical or logical methods. When a sensitive application is to run in a shared environment, the application systems with which it will share resources and the corresponding risks are identified and accepted by the owner of the sensitive application.
Level 2 Control Standard Mapping:	CMMC v1.0 SC.4.197-0 CRR v2016 CM:G2.Q2 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 PR.AC-5 NIST Cybersecurity Framework v1.1 PR.DS-5

Level 3 Implementation Requirements

Level 3 Organizational Factors:	
Level 3 System Factors:	Number of users of the system(s) Greater than 5,500

Level 3 Regulatory Factors:	Subject to CMMC Level 3 Subject to FedRAMP Certification Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: Users of shared system resources cannot intentionally or unintentionally access information remnants, including encrypted representations of information, produced by the actions of a prior user or system process acting on behalf of a prior user. System resources shared between two or more users are released back to the information system and are protected from accidental or purposeful disclosure. Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS are implemented on separate servers.) If virtualization technologies are used, verify that one component or primary function is implemented per virtual system device. The information system maintains a separate execution domain for each executing process.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMMC v1.0 SC.3.182-1 CMSRs v3.1 SC-04 (HIGH; MOD) FedRAMP SC-4 IRS Pub 1075 v2016 9.3.16.3 IRS Pub 1075 v2016 9.4.1 MARS-E v2 SC-4 NIST 800-171 r2 3.13.4-1 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST SP 800-53 R4 SC-3(1)[S]{0} NIST SP 800-53 R4 SC-39(1)[S]{0} NIST SP 800-53 R4 SC-39(2)[S]{0} NIST SP 800-53 R4 SC-39[HML]{0} NIST SP 800-53 R4 SC-4[HM]{0} NY DOH SSP v3.1 SC-39[M]-0 NY DOH SSP v3.1 SC-4.IS1[M]-0 NY DOH SSP v3.1 SC-4[M]-0

Level CMS Implementation Requirements

Level CMS Implementation:	The organization employs boundary protection mechanisms to separate defined information system components (defined in the applicable security plan) supporting CMS missions and/or business functions. The organization ensures that system resources shared between two or more users are released back to the information system and are protected from accidental or purposeful disclosure.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	When an authorization to make further disclosures is present (e.g., agents/contractors), information disclosed outside the organization must be recorded on a separate list that reflects to whom the disclosure was made, what was disclosed, and why and when it was disclosed. Organizations transmitting FTI from one computer to another need only identify the bulk records transmitted. This identification will contain the approximate number of personal records, the date of the transmissions, the best possible description of the records, and the name of the individual making/receiving the transmission. Software, data, and services that receive, process, store, or transmit FTI must be isolated within a cloud environment so that other cloud customers sharing physical or virtual space cannot access other customer data or applications.

Level HIX	Implementation Requirements
Level HIX Implementation:	The organization ensures that system resources shared between two or more users are released back to the information system and are protected from accidental or purposeful disclosure.

Level Supplemental Requirements	Implementation Requirements
Level Supplemental Requirements Implementation:	Sensitive applications and information must be segregated from any other customer's or supplier's own application or information by using logical access controls and/or physical access controls.

Objective Name: 01.07 Mobile Computing and Teleworking

Control Objective:	To ensure the security of information when using mobile computing devices and teleworking facilities.

Control Reference: 01.x Mobile Computing and Communications

Control Specification:	A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication devices. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Communications and Transmissions; Cryptography; Data Loss Prevention; Media and Assets; Physical and Facility Security; Policies and Procedures; Network Security

Level 1	Implementation Requirements
Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 3 Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance

	Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to State of Massachusetts Data Protection Act Subject to Supplemental Requirements Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	The organization uses full-disk encryption to protect the confidentiality of information on laptops and other mobile devices that support full-disk encryption. Encryption is required for all other mobile computing devices in accordance with the organization's data protection policy (see 06.d) and enforced through technical controls. If it is determined that encryption is not reasonable and appropriate, the organization documents its rationale and acceptance of risk. A mobile computing policy is developed and include the organization's definition of mobile devices, acceptable usage, and the requirements for physical protection, access controls, cryptographic techniques, back-ups, and virus protection. This policy also includes rules and advice on connecting mobile devices to networks and guidance on the use of these devices in public places. Protection is in place when using mobile computing devices in public places, meeting rooms and other unprotected areas outside of the organization's premises to avoid the unauthorized access to or disclosure of the information stored and processed by these devices (e.g., using cryptographic techniques). Users of mobile computing devices in public places are to take care to avoid the risk of overlooking by unauthorized persons. The organization installs personal firewall software or equivalent functionality on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network. Suitable protection is given to the use of mobile devices connected to networks. The organization only authorizes connections of mobile devices meeting organizational usage restrictions, configuration requirements, connection requirements, and implementation guidance; enforces requirements for the connection of mobile devices to sensitive information systems; and monitors for unauthorized connections. Information system functionality on mobile devices that provides the capability for automatic execution of code without user direction is disabled. Individuals are issued specifically configured mobile devices for travel to locations the organization deems to be of significant risk in accordance with organizational policies and procedures. The devices are checked for malware and physical tampering upon return from these locations. Mobile computing devices are also physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centers, and meeting places. A specific procedure taking into account legal, insurance and other security requirements of the organization is established for cases of theft or loss of the mobile computing devices. Equipment carrying important, covered, and/or critical business information is not to be left unattended without being physically protected. Training is arranged for personnel using mobile computing to raise their awareness on the additional risks resulting from this way of working and the controls that need to be implemented.

	A documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing entity (client) or cloud service provider-managed client data, and the use of unapproved application stores is prohibited for company-owned and BYOD mobile devices. The installation of non-approved applications or approved applications not obtained through a pre-identified application store is prohibited. The organization prohibits the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting).
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) CIS CSC v7.1 13.6 CIS CSC v7.1 8.1 CMMC v1.0 AC.3.020-0 CMMC v1.0 AC.3.022-0 CMSRs v3.1 AC-19 (HIGH; MOD) CMSRs v3.1 AC-19(05) (HIGH; MOD) CMSRs v3.1 CM-02(07) (HIGH; MOD) CMSRs v3.1 SI-04 (HIGH; MOD) CSA CCM v3.0.1 HRS-05 CSA CCM v3.0.1 MOS-02 CSA CCM v3.0.1 MOS-03 CSA CCM v3.0.1 MOS-05 CSA CCM v3.0.1 MOS-10 CSA CCM v3.0.1 MOS-11 CSA CCM v3.0.1 MOS-12 CSA CCM v3.0.1 MOS-17 CSA CCM v3.0.1 MOS-18 CSA CCM v3.0.1 MOS-19 FedRAMP AC-19 FedRAMP AC-19(5) FedRAMP CM-2(7) FedRAMP SC-7(12) FFIEC IS v2016 A.6.24 IRS Pub 1075 v2016 4.5 IRS Pub 1075 v2016 9.3.1.14 IRS Pub 1075 v2016 9.4.8 ISO/IEC 27002:2013 6.2.1 ISO/IEC 27799:2016 6.2.1 MARS-E v2 AC-19 MARS-E v2 AC-19(5) MARS-E v2 SC-7(12) NIST 800-171 r2 3.1.18-0 NIST 800-171 r2 3.1.19-0 NIST Cybersecurity Framework v1.1 DE.CM-7 NIST Cybersecurity Framework v1.1 PR.AC-2 NIST Cybersecurity Framework v1.1 PR.AT-1 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.IP-1 NIST SP 800-53 R4 AC-19(4)a[S]{2} NIST SP 800-53 R4 AC-19(4)b[S]{1} NIST SP 800-53 R4 AC-19(4)b[S]{5} NIST SP 800-53 R4 AC-19(4)c[S]{0} NIST SP 800-53 R4 AC-19(5)[HM]{0} NIST SP 800-53 R4 AC-19[HML]{0} NIST SP 800-53 R4 CM-2(7)[HM]{0} NIST SP 800-53 R4 MP-7(2)[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 AC-19a[M]-0 NY DOH SSP v3.1 CM-2(7)a[M]-1 NY DOH SSP v3.1 CM-2(7)b[M]-1 PCI DSS v3.2.1 1.4 PCI DSS v3.2.1 9.5 PMI DSP Framework PR.DS-1 SR v6.4 38a-0 SR v6.4 38b-0 SR v6.4 38d-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Supplemental Requirements
Level 2 Implementation:	A centralized, mobile device management solution is deployed to all mobile devices permitted to store, transmit, or process organizational and/or customer data. Prohibition on the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) is enforced through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management) including enabling secure containers and or sandbox solutions. All mobile devices permitted for use through the company BYOD program, or a company-assigned mobile device allow for remote wipe by the company's corporate IT or have all company-provided data wiped by the company's corporate IT. Mobile devices connecting to corporate networks, or storing and accessing company information, allow for remote software version/patch validation. All mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel are able to perform these updates remotely.
Level 2 Control Standard Mapping:	CIS CSC v7.1 12.12 CSA CCM v3.0.1 MOS-10 CSA CCM v3.0.1 MOS-12 CSA CCM v3.0.1 MOS-18 CSA CCM v3.0.1 MOS-19 FFIEC IS v2016 A.6.24 NIST SP 800-53 R4 AC-19(4)b[S]{3} NIST SP 800-53 R4 SA-18(2)[S]{1} NY DOH SSP v3.1 MP-6(8)[MN]-0 SR v6.4 38c-0 SR v6.4 39a-0 SR v6.4 39b-0

Level CMS Implementation Requirements

Level CMS Implementation:	The organization ensures the CIO authorizes the connection of mobile devices to organizational information systems.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	Purge/wipe information from mobile devices based on 10 consecutive, unsuccessful device logon attempts (e.g., personal digital assistants, smartphones and tablets). Laptop computers are excluded from this requirement. To use FTI in a mobile device environment, including BYOD, the agency must meet the following mandatory requirements: 1. Mobile device management controls must be in place that include security policies and procedures, inventory, and standardized security configurations for all devices; 2. An annual risk assessment must be conducted of the security controls in place on all devices in the mobile environment used for receiving, processing, storing, or transmitting FTI; 3. Protection mechanisms must be in place in case a mobile device is lost or stolen, e.g., all data stored on the device must be encrypted, including internal storage and removable media storage, such as Micro Secure Digital (SD) cards; 4. All data communication with the agency's internal network must be encrypted using a cryptographic module that is FIPS 140-2 compliant; 5. The agency must control end user ability to download only authorized applications to the device and must limit the accessibility to FTI by applications to only authorized applications; 6. All mobile device management servers that receive, process, store, or transmit FTI must be hardened; 7. A centralized mobile device management solution must be used to authenticate agency-issued and personally-owned mobile devices prior to allowing access to the internal network 8. Security events must be logged for all mobile devices and the mobile device management server; 9. The agency must disable wireless personal area networks that allow a mobile device to connect to a computer via Bluetooth or near field communication (NFC) for data synchronization and storage; 10. Access to hardware, such as the digital camera, global positioning system (GPS), and universal serial bus (USB) interface, must be disabled to the extent possible; and 11. Disposal of all mobile device component hardware follows the same media sanitization and disposal procedures as other media.

Level HIX Implementation Requirements

Level HIX Implementation:	If the connection of portable and mobile devices is authorized, the organization: 1. Authorizes the connection of mobile devices to organizational information systems through the CIO; 2. Only allows the use of organization-owned mobile devices and software to process, access, and store Personally Identifiable Information (PII); 3. Employs an approved method of cryptography (see SC-13) to protect information residing on portable and mobile information devices, and utilizes whole-disk encryption solution for laptops; 4. Monitors for unauthorized connections of mobile devices to information systems; 5. Enforces requirements for the connection of mobile devices to information systems; 6. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and 7. Protects the storage and transmission of information on portable and mobile information devices with activities such as scanning the devices for malicious code, virus protection software.

	Purge/wipe information from mobile devices based on ten consecutive, unsuccessful device logon attempts (e.g., personal digital assistants, smartphones, and tablets, but laptop computers are excluded from this requirement).

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The information system purges/wipes information from organization-defined mobile devices based on organization-defined purging/wiping requirements/techniques after an organization-defined number of consecutive, unsuccessful device logon attempts. Full disk encryption is required for all State-issued laptops that access or contain SE information; full disk encryption products must use either pre-boot authentication that utilizes the device's Trusted Platform Module (TPM), or Unified Extensible Firmware Interface (UEFI) Secure Boot.

Control Reference: 01.y Teleworking

Control Specification:	A policy, operational plans and procedures shall be developed and implemented for teleworking activities. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Authorization; Communications and Transmissions; IT Organization and Management Roles and Responsibilities; Media and Assets; Personnel; User Access; Network Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 3 Subject to FISMA Compliance Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline
Level 1 Implementation:	Organizations only authorize teleworking activities if they are satisfied that appropriate security arrangements and controls are in place, and that these comply with the organization's security policy. Suitable protection of the teleworking site is in place to protect against the theft of equipment and information, the unauthorized disclosure of information, unauthorized remote access to the organization's internal systems or misuse of facilities. The following matters are addressed: 1. the communications security requirements, taking into account the need for remote access to the organization's internal systems, the sensitivity of the information that will be accessed and pass over the communication link, and the sensitivity of the internal system;

	2. the use of home networks and requirements or restrictions on the configuration of wireless network services including encryption (AES WPA2, at a minimum); 3. anti-virus protection, operating system and application patching, and firewall requirements consistent with corporate policy; and 4. revocation of authority and access rights, and the return of equipment when the teleworking activities are terminated. Verifiable unique IDs are required for all teleworkers accessing the organization's network via a remote connection. The connection between the organization and the teleworker's location is secured via an encrypted channel. The organization maintains ownership over the assets used by the teleworker in order to achieve the requirements of this control (e.g., issuance of a USB device to allow for remote access via an encrypted tunnel). Teleworking activities are both authorized and controlled by management and ensured that suitable arrangements are in place for this way of working. Training on security awareness, privacy and teleworker responsibilities is required prior to authorization and training methods are reviewed in accordance with the organization's policy (see 02.e).
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) CMMC v1.0 PE.3.136-1 CMSRs v3.1 AC-17 (HIGH; MOD) CMSRs v3.1 AC-17(02) (HIGH; MOD) CMSRs v3.1 AT-02 (HIGH; MOD) CMSRs v3.1 IA-02 (HIGH; MOD) CMSRs v3.1 PE-17 (HIGH; MOD) FedRAMP AC-17 FedRAMP AC-17(2) FedRAMP AT-2 FedRAMP IA-2 FedRAMP PE-17 FFIEC IS v2016 A.6.23 FFIEC IS v2016 A.6.24 IRS Pub 1075 v2016 4.7.1 IRS Pub 1075 v2016 9.3.1.12 ISO/IEC 27002:2013 6.2.1 ISO/IEC 27002:2013 6.2.2 ISO/IEC 27799:2016 6.2.1 ISO/IEC 27799:2016 6.2.2 MARS-E v2 AC-17 MARS-E v2 AC-17(2) MARS-E v2 AT-2 MARS-E v2 IA-2 MARS-E v2 PE-17 NIST 800-171 r2 3.10.6-1 NIST Cybersecurity Framework v1.1 PR.AC-2 NIST Cybersecurity Framework v1.1 PR.AC-3 NIST Cybersecurity Framework v1.1 PR.AT-1 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.DS-2 NIST Cybersecurity Framework v1.1 PR.DS-3 NIST Cybersecurity Framework v1.1 PR.IP-1 NIST SP 800-53 R4 AC-17a[HML]{2} NIST SP 800-53 R4 PE-17b[HM]{0} NY DOH SSP v3.1 PE-17a[M]-2 PMI DSP Framework PR.IP-2

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians

	Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to NY OHIP Moderate-Plus Security Baseline
Level 2 Implementation:	Level 1 plus: The following matters are addressed prior to authorizing teleworking: 1. the existing physical security of the teleworking site, taking into account the physical security of the building and the local environment; 2. the proposed physical teleworking environment; and 3. the threat of unauthorized access to information or resources from other persons using the accommodation (e.g., family and friends).
Level 2 Control Standard Mapping:	NIST Cybersecurity Framework v1.1 PR.AC-2 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.IP-1 NY DOH SSP v3.1 PE-17b[M]-0

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to EHNAC Accreditation Subject to FedRAMP Certification Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: The following matters are addressed prior to authorizing teleworking: 1. a definition of the work permitted, the hours of work, the classification of information that may be held, and the internal systems and services that the teleworker is authorized to access;

	2. the provision of suitable equipment and storage furniture for the teleworking activities, where the use of privately owned equipment that is not under the control of the organization is not allowed; 3. the provision of suitable communication equipment, including methods for securing remote access; 4. rules and guidance on family and visitor access to equipment and information; 5. the provision of hardware and software support and maintenance; 6. the provision of insurance; 7. the procedures for back-up and business continuity; 8. the provision of a means for teleworkers to communicate with information security personnel in case of security incidents or problems; and 9. audit and security monitoring. The organization instructs all personnel working from home to implement fundamental security controls and practices, including but not limited to passwords, virus protection, personal firewalls, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems at alternate worksites. Remote access is limited to only information resources required by home users to complete job duties. Any organization-owned equipment is only used only for business purposes by authorized employees.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 AC-06 (HIGH; MOD) CMSRs v3.1 AC-20 (HIGH; MOD) CMSRs v3.1 PE-17 (HIGH; MOD) FedRAMP AC-20 FedRAMP AC-6 FedRAMP PE-17 IRS Pub 1075 v2016 4.5 IRS Pub 1075 v2016 4.7 IRS Pub 1075 v2016 4.7.1 IRS Pub 1075 v2016 4.7.2 IRS Pub 1075 v2016 9.3.1.6 IRS Pub 1075 v2016 9.3.11.9 ISO/IEC 27002:2013 6.2.2 ISO/IEC 27799:2016 6.2.2 MARS-E v2 AC-20 MARS-E v2 AC-6 MARS-E v2 PE-17 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 PR.AC-2 NIST Cybersecurity Framework v1.1 PR.AC-3 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.IP-1 NIST SP 800-53 R4 AC-17b[HML]{0} NIST SP 800-53 R4 AU-14(3)[S]{1} NIST SP 800-53 R4 PE-17a[HM]{0} NIST SP 800-53 R4 PE-17c[HM]{2} NY DOH SSP v3.1 AC-17.IS4b[M]-0 NY DOH SSP v3.1 AC-17.IS4c[M]-0 NY DOH SSP v3.1 AC-17a[M]-2 NY DOH SSP v3.1 AC-20.IS1[M]-1 NY DOH SSP v3.1 AC-20.IS1[M]-2 NY DOH SSP v3.1 PE-17a[M]-1 NY DOH SSP v3.1 PE-17c[M]-0

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	If the agency allows alternative work sites, such as an employee's home or other non-traditional work sites, the FTI remains subject to the same safeguard requirements as the agency's offices and the highest level of attainable security (see also IRS Pub 1075 v2014 4.5). The organization addresses how it will meet its minimum protection standards for FTI at alternate worksites (e.g., employee's homes or other non-traditional work sites).

	The agency conducts and fully documents periodic inspections of alternative work sites during the year to ensure that safeguards are adequate. The agency must retain ownership and control, for all hardware, software, and end-point equipment connecting to public communication networks, where these are resident at all alternate work sites. Employees must have a specific room or area in a room that has the appropriate space and facilities for the type of work done. The agency must give employees locking file cabinets or desk drawers so that documents, disks, and tax returns may be properly secured when not in use. If agency furniture is not furnished to the employee, the agency must ensure that an adequate means of storage exists at the work site. The agency must provide locking hardware to secure automated data processing equipment to large objects, such as desks or tables. Smaller, agency-owned equipment must be locked in a filing cabinet or desk drawer when not in use. FTI may be stored on hard disks only if agency-approved security access control devices (hardware/software) have been installed; are receiving regularly scheduled maintenance, including upgrades; and are being used. Access control must include password security, an audit trail, encryption, virus detection, and data overwriting capabilities. Computers and electronic media that receive, process, store, or transmit FTI must be in a secure area with restricted access. In situations when requirements of a secure area with restricted access cannot be maintained, such as home-work sites, remote terminals or other office work sites, the equipment must receive the highest level of protection practical, including full disk encryption. All computers and mobile devices that contain FTI and are resident in an alternate work site must employ encryption mechanisms to ensure that this data may not be accessed if the computer is lost or stolen.

Control Category: 02.0 - Human Resources Security

Objective Name: 02.01 Prior to Employment

Control Objective:	To ensure that employees, contractors, and third-party users are suitable for the roles for which they are being considered, to reduce the risk of fraud, theft, or misuse of facilities.

Control Reference: 02.a Roles and Responsibilities

Control Specification:	Security roles and responsibilities of employees, contractors and third-party users shall be defined and documented in accordance with the organization's information security policy. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Awareness and Training; Incident Response; IT Organization and Management Roles and Responsibilities; Personnel; Policies and Procedures

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to PCI Compliance
Level 1 Implementation:	The organization develops, disseminates, and reviews/updates annually: 1. a formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls. Security roles and responsibilities include the following requirements: 1. implement and act in accordance with the organization's information security policies; 2. protect assets from unauthorized access, disclosure, modification, destruction, or interference; 3. execute particular security processes or activities; 4. ensure responsibility is assigned to the individual for actions taken; and 5. report security events or potential events or other security risks to the organization. Security roles and responsibilities are defined and clearly communicated to job candidates during the pre-employment process. Security roles and responsibilities, as laid down in the organization's information security policy, as well as any involvement in processing covered information documented in relevant job descriptions.

Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC1.4 CMSRs v3.1 PS-01 (HIGH; MOD) CRR v2016 CCM:MIL3.Q2 CRR v2016 CM:G2.Q9 CRR v2016 CM:MIL3.Q2 CRR v2016 EDM:MIL3.Q2 CRR v2016 RM:MIL3.Q2 CRR v2016 SCM:MIL3.Q2 CRR v2016 VM:MIL3.Q2 CSA CCM v3.0.1 HRS-07 FedRAMP AC-1 FedRAMP PS-1 FFIEC IS v2016 A.2.7 FFIEC IS v2016 A.2.9 IRS Pub 1075 v2016 9.3.13.1 ISO/IEC 27002:2013 6.1.1 ISO/IEC 27002:2013 7.1.2 ISO/IEC 27799:2016 6.1.1 ISO/IEC 27799:2016 7.1.2 MARS-E v2 PS-1 NIST Cybersecurity Framework v1.1 DE.DP-1 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 PR.IP-11 NRS 603A.215.1 PCI DSS v3.2.1 12.4.1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The pre-employment process is reviewed by recruitment to ensure security roles and responsibilities are defined and clearly communicated to job candidates. The organization assigns risk designations to all organizational positions as appropriate, establishes screening criteria, and reviews and revises designations every 365 days.

	The organization defines the roles, responsibilities, and authority of all security personnel.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 PS-02 (HIGH; MOD) CRR v2016 CM:G2.Q9 FedRAMP PS-2 FFIEC IS v2016 A.2.7 FFIEC IS v2016 A.2.9 IRS Pub 1075 v2016 9.3.13.2 ISO/IEC 27002:2013 7.1.2 ISO/IEC 27799:2016 7.1.2 MARS-E v2 PS-2 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 PS-2[HML]{0} NIST SP 800-53 R4 PS-3(3)b[S]{0} NIST SP 800-53 R4 PS-6(2)c[S]{2} NIST SP 800-53 R4 SA-21(1)[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 PS-2a[M]-0 NY DOH SSP v3.1 PS-2b[M]-0 NY DOH SSP v3.1 PS-2e[M]-0 PCI DSS v3.2.1 12.4.1

Level DGF Implementation Requirements

Level DGF Implementation:	Data Governance roles and responsibilities such as Data Producers, Data Consumers, Data Custodians, Data Stewards, and stakeholders are defined and documented.

Control Reference: 02.b Screening

Control Specification:	Background verification checks on all candidates for employment, contractors, and third-party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.
Factor Type:	Organizational
Topics:	Authorization; IT Organization and Management Roles and Responsibilities; Personnel; Requirements (Legal and Contractual); Third-parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 2 Subject to NIST 800-171 Basic Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance
Level 1 Implementation:	The organization screens individuals requiring access to organizational information and before authorizing access.

	Verification checks take into account all relevant privacy, protection of covered data and/or employment-based legislation, and where permitted and appropriate, include the following: 1. availability of satisfactory character references (e.g., one business and one personal); 2. a check (for completeness and accuracy) of the applicant's curriculum vitae; 3. confirmation of claimed academic and professional qualifications; and 4. independent identity check (passport or similar document). All applicants are required to complete an I-9 form to verify that they are eligible to work in the United States and to verify their identity prior to granting access to covered information. Where a job, either on initial appointment or on promotion, involves the person having access to information assets, and in particular those handling covered information (e.g., financial information, personal health information or highly confidential information) the organization, at a minimum, verifies the identity, current address (for initial appointment) and previous employment of such staff prior to granting or continuing access, including the contribution of covered information. Procedures define criteria and limitations for verification checks (e.g., who is eligible to screen people, and how, when, and why verification checks are carried out). Information on all candidates being considered for positions within the organization is collected and handled in accordance with any appropriate legislation existing in the relevant jurisdiction. Depending on applicable legislation, the candidates are informed beforehand about the screening activities.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) CMMC v1.0 PS.2.127-0 CMSRs v3.1 PS-01 (HIGH; MOD) CMSRs v3.1 PS-02 (HIGH; MOD) CMSRs v3.1 PS-03 (HIGH; MOD) CRR v2016 CM:G2.Q9 CSA CCM v3.0.1 HRS-02 FedRAMP PS-1 FedRAMP PS-2 FedRAMP PS-3 FFIEC IS v2016 A.6.8(b) HITRUST IRS Pub 1075 v2016 9.3.13.2 IRS Pub 1075 v2016 9.3.13.3 IRS Pub 1075 v2016 Exhibit 10 ISO/IEC 27002:2013 7.1.1 ISO/IEC 27799:2016 7.1.1 MARS-E v2 PS-1 MARS-E v2 PS-2 MARS-E v2 PS-3 NIST 800-171 r2 3.9.1-0 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 IA-4(3)[S]{1} NIST SP 800-53 R4 PS-3a[HML]{0} NIST SP 800-53 R4 SA-21[S]{2} NRS 603A.215.1 NY DOH SSP v3.1 IA-4(3)[MN]-0 NY DOH SSP v3.1 PS-3a[M]-0 NY DOH SSP v3.1 PS-3e1[M]-0 PCI DSS v3.2.1 12.7 PMI DSP Framework PR.AC-1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions

	Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to CRR V2016 Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The organization has an HR representative as a single point of contact for performing the screening process on applicants. The organization develops a standard criteria screening process to be carried out on all applicants. The organization assigns risk designation to all positions and established criteria for individuals filling those positions. Applicants are screened in accordance with applicable regional policies/procedures that may require screening in the following areas: 1. health screening; 2. drug screening; and 3. motor vehicle driving record (in accordance with job requirements). Criminal background checks are undertaken prior to employment. The organization rescreens individuals periodically, consistent with the criticality/sensitivity rating of the position and, when an employee moves from one position to another, any higher level of access (clearance) is adjudicated. The organization considers applicable state and federal law (reference 02.b, level 1) with regards to information exchanged in the notification process with business partners, vendors and other applicable third-parties described in 05.k, level 1, which is meant to ensure third-party workforce members pass verification checks prior to employment. If there has been a long gap, at a minimum five years, between recruitment and the date of the employee starting, the organization repeats the screening process, or its key elements.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC1.4 CMSRs v3.1 PS-01 (HIGH; MOD) CMSRs v3.1 PS-02 (HIGH; MOD) CMSRs v3.1 PS-03 (HIGH; MOD) CRR v2016 CM:G2.Q9 FedRAMP PS-1 FedRAMP PS-2 FedRAMP PS-3 FFIEC IS v2016 A.6.8(b) IRS Pub 1075 v2016 9.3.13.2 IRS Pub 1075 v2016 9.3.13.3

	IRS Pub 1075 v2016 Exhibit 10 ISO/IEC 27002:2013 7.1.1 ISO/IEC 27799:2016 7.1.1 MARS-E v2 PS-1 MARS-E v2 PS-2 MARS-E v2 PS-3 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 PS-3b[HML]{0} NIST SP 800-53 R4 SI-12[HML]{2} NRS 603A.215.1 NY DOH SSP v3.1 PS-2.PII[M]-1 NY DOH SSP v3.1 PS-2d[M]-0 NY DOH SSP v3.1 PS-3(3)b[MN]-0 NY DOH SSP v3.1 PS-3b[M]-0 PCI DSS v3.2.1 12.7

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to Banking Requirements Subject to FedRAMP Certification Subject to NY OHIP Moderate-Plus Security Baseline
Level 3 Implementation:	Level 2 plus: The organization specifically defines an individual who performs all screening checks. The organization documents and maintains a list of all screened applicants with assigned risk. Credit checks are carried out for personnel who will have access to financial information.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 PS-03 (HIGH; MOD) FedRAMP PS-3 FedRAMP PS-3(3) FFIEC IS v2016 A.6.8(b) IRS Pub 1075 v2016 9.3.13.3 ISO/IEC 27002:2013 7.1.1 ISO/IEC 27799:2016 7.1.1 MARS-E v2 PS-3 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 PR.IP-11 NY DOH SSP v3.1 PS-2.PII[M]-2 PCI DSS v3.2.1 12.7

Level CMS Implementation Requirements

Level CMS Implementation:	Require that individuals with significant security responsibilities be assigned and hold, at a minimum, Tier 2S background investigation as defined in the HHS Personnel Security/Suitability Handbook. Assign other individuals with Public Trust positions the

	appropriate sensitivity level as defined in the HHS Personnel Security/Suitability Handbook.

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation:	Rescreening is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the fifth year.

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation:	Individuals must be screened before authorizing access to information systems and devices containing FTI. Organizations consider additional background checks for staff members with administrator access to the entire set of FTI records.

Objective Name: 02.02 During On-Boarding

Control Objective:	To ensure agreements are signed by employees, contractors, and third-party users of information assets on their security roles and responsibilities at the time of their employment or engagement, prior to access being granted.

Control Reference: 02.c Terms and Conditions of Employment

Control Specification:	As part of their contractual obligation, employees, contractors, and third-party users shall agree and sign the terms and conditions of their employment contract, which shall include their responsibilities for information security.
Factor Type:	Organizational
Topics:	Documentation and Records; IT Organization and Management Roles and Responsibilities; Personnel; Requirements (Legal and Contractual); Third-parties and Contractors

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)

Level 1 Implementation:	The terms and conditions of employment reflect the organization's security policy, in addition to clarifying and stating the following: 1. that all employees, contractors, and third-party users who are given access to covered information sign a confidentiality or non-disclosure agreement prior to being given access to information assets; 2. the employee's, contractor's and any other user's legal responsibilities and rights (e.g., regarding copyright laws or data protection legislation); 3. responsibilities for the classification of information and management of organizational assets associated with information systems and services handled by the employee, contractor or third-party user; 4. responsibilities of the employee, contractor, or third-party user for the handling of information received from other companies or external parties; 5. responsibilities of the organization for the handling of covered information, including covered information created as a result of, or in the course of, employment with the organization; 6. responsibilities that are extended outside the organization's premises and outside normal working hours (e.g., in the case of home-working); 7. actions to be taken if the employee, contractor, or third-party user disregards the organization's security requirements; and 8. ensure that conditions relating to security policy survive the completion of the employment in perpetuity. The organization ensures that employees, contractors, and third-party users agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services. The organization develops and documents access agreements for organizational systems and privileges are not granted until the terms and conditions of employment have been satisfied and agreements have been signed.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC1.4 CMSRs v3.1 PL-04 (HIGH; MOD) CMSRs v3.1 PS-06 (HIGH; MOD) CSA CCM v3.0.1 HRS-03 FedRAMP PL-4 FedRAMP PS-6 FFIEC IS v2016 A.2.7 FFIEC IS v2016 A.2.9 IRS Pub 1075 v2016 9.3.12.3 IRS Pub 1075 v2016 9.3.13.6 ISO/IEC 27002:2013 7.1.2 ISO/IEC 27799:2016 7.1.2 MARS-E v2 PL-4 MARS-E v2 PS-6 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 PS-4(1)b[S]{1} NIST SP 800-53 R4 PS-6(3)b[S]{0} NIST SP 800-53 R4 PS-6a[HML]{1} NIST SP 800-53 R4 PS-6c[HML]{1} NIST SP 800-53 R4 SA-21[S]{1} NRS 603A.215.1 NY DOH SSP v3.1 PS-6a[M]-0 NY DOH SSP v3.1 PS-6c1[M]-0 PCI DSS v3.2.1 12.4

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to HITRUST De-ID Framework Requirements
Level 2 Implementation:	Level 1 plus: The organization maintains a list of all authorized signed non-disclosure agreement (NDA) forms. This list is kept up to date to reflect personnel or other workforce member changes and departures. Responsibilities contained within the terms and conditions of employment continue for a defined period after the end of the employment. The terms and conditions of employment: 1. include reference to the penalties that are possible when breach of the information security policy is identified; 2. ensure that conditions relating to confidentiality of covered information (e.g., PII) survive the completion of the employment for the maximum period allowed under applicable federal and state laws and regulations. With respect to clinical staff, the terms and conditions of employment specify what rights of access such staff will have to the records of subjects of care and to the associated health information systems in the event of third-party claims.
Level 2 Control Standard Mapping:	De-ID Framework v1 Non-disclosure and Confidentiality: Policy ISO/IEC 27002:2013 7.1.2 ISO/IEC 27799:2016 7.1.2 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 PR.IP-11

Level CMS Implementation Requirements

Level CMS Implementation:	The organization reviews/updates the access agreements as part of the system security authorization or when a contract is renewed or extended, but minimally within every 365 days, whichever occurs first. The organization ensures that individuals requiring access to organizational information or information systems sign appropriate access agreements prior to being granted access and re-acknowledge such agreements when they are updated, or within 365 days, to maintain access to organizational information systems.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The organization reviews/updates the access agreements within every 365 days.

	The organization ensures that individuals requiring access to organizational information or information systems sign appropriate access agreements prior to being granted access and re-acknowledge such agreements when they are updated to maintain access to organizational information systems. The organization requires third-party providers to notify organization-defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges, within the same day.

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation:	Agencies must review information system access authorizations and initiate appropriate actions when personnel are reassigned or transferred to other positions within the organization.

Level HIPAA Implementation Requirements	
Level HIPAA Implementation:	With respect to clinical staff, the terms and conditions of employment specify what rights of access such staff will have to the records of subjects of care and to the associated health information systems in the event of third-party claims. The terms and conditions of employment: 1. include reference to the penalties that are possible when breach of the information security policy is identified; 2. ensure that conditions relating to confidentiality of personal health information survive the completion of the employment for the maximum period allowed under applicable federal and state laws and regulations.

Objective Name: 02.03 During Employment

Control Objective:	To ensure that employees, contractors, and third-party users are aware of information security threats and concerns, their responsibilities, and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

Control Reference: 02.d Management Responsibilities

Control Specification:	Management shall require employees, and where applicable, contractors and third-party users, to apply security in accordance with established policies and procedures of the organization. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	IT Organization and Management Roles and Responsibilities; Personnel; Policies and Procedures; Third-parties and Contractors

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Applicable to all Organizations

Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to HIPAA Security Rule Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline
Level 1 Implementation:	Management responsibilities include ensuring that employees, contractors, and third-party users: 1. are properly briefed on their information security roles and responsibilities prior to being granted access to covered and/or confidential information or information systems; 2. are provided with guidelines to state security expectations of their role within the organization; 3. are motivated and comply with the security policies of the organization; 4. achieve a level of awareness on security relevant to their roles and responsibilities within the organization; 5. conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working; and 6. continue to have the appropriate skills and qualifications. The organization establishes an information security workforce development and improvement program. The organization: 1. implements a process for ensuring that organization plans for conducting security testing, training, and monitoring activities associated with organizational information systems: i. are developed and maintained; and ii. continue to be executed in a timely manner; 2. reviews testing, training, and monitoring plans for consistency with the organization risk management strategy and organization-wide priorities for risk response actions. The organization develops usage policies for critical employee-facing technologies to define proper use of these technologies for all employees and contractors.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.308(a)(3)(ii)(A) HIPAA.SR-1 AICPA 2017 CC1.2 AICPA 2017 CC1.4 AICPA 2017 CC2.2 AICPA 2017 CC3.2 CMSRs v3.1 AT-03 (HIGH; MOD) CMSRs v3.1 PM-13 (HIGH; MOD) CMSRs v3.1 PM-14 (HIGH; MOD) CMSRs v3.1 PM-15 (HIGH; MOD) CRR v2016 AM:G6.Q4 CRR v2016 AM:MIL3.Q2 CRR v2016 CCM:MIL3.Q2 CRR v2016 CM:MIL3.Q2 CRR v2016 EDM:MIL3.Q2 CRR v2016 IM:MIL3.Q2 CRR v2016 RM:MIL3.Q2 CRR v2016 SA:G1.Q2 CRR v2016 SA:G3.Q3 CRR v2016 SA:MIL3.Q2 CRR v2016 SCM:MIL3.Q2

	CRR v2016 TA:G1.Q2 CRR v2016 TA:MIL2.Q2 CRR v2016 TA:MIL3.Q2 CRR v2016 TA:MIL4.Q2 CRR v2016 VM:MIL3.Q2 CSA CCM v3.0.1 GRM-03 CSA CCM v3.0.1 HRS-10 FedRAMP AT-3 FedRAMP PS-7 FFIEC IS v2016 A.2.10 FFIEC IS v2016 A.2.7 FFIEC IS v2016 A.2.9 IRS Pub 1075 v2016 9.3.13.7 IRS Pub 1075 v2016 9.3.2.3 IRS Pub 1075 v2016 Exhibit 10 ISO/IEC 27002:2013 7.2.1 ISO/IEC 27799:2016 7.2.1 MARS-E v2 AT-3 MARS-E v2 PM-13 MARS-E v2 PM-14 MARS-E v2 PM-15 MARS-E v2 PS-7 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 PR.AT-1 NIST Cybersecurity Framework v1.1 PR.AT-2 NIST Cybersecurity Framework v1.1 PR.AT-3 NIST Cybersecurity Framework v1.1 PR.AT-4 NIST Cybersecurity Framework v1.1 PR.AT-5 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 PM-14[HML]{0} NIST SP 800-53 R4 PS-3(1)[S]{0} NIST SP 800-53 R4 PS-3(2)[S]{1} NIST SP 800-53 R4 SA-17(6)[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 CA-8.IS5[ML]-0 NY DOH SSP v3.1 PM-13[M]-0 NY DOH SSP v3.1 PM-14a1[M]-0 NY DOH SSP v3.1 PM-14a2[M]-0 NY DOH SSP v3.1 PM-14b[M]-0 NY DOH SSP v3.1 PM-1a[M]-2 NY DOH SSP v3.1 SI-4(4)[M]-2 NY DOH SSP v3.1 SI-4b[M]-3 PCI DSS v3.2.1 12.3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (Supplemental) Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)

Level 2 Implementation:	Level 1 plus: The organization assigns an individual or team to manage information security responsibilities of employees, contractors, and third-party users. For all system connections that allow customers to access the computing assets such as websites, kiosks and public access terminals, the organization ensures the following: 1. provides appropriate text or a link to the privacy policy for data use and protection as well as the customer's responsibilities when accessing the data; and 2. has a formal mechanism to authenticate the customer's identity prior to granting access to covered information. These usage policies address the following if applicable: 1. explicit management approval (authorization) to use the technology; 2. authentication for use of the technology; 3. acceptable uses of the technologies (see 07.c), with special emphasis on the inappropriate access by health workers of personal health information of neighbors, colleagues, and relatives; 4. acceptable network locations for the technologies; 5. list of company-approved products; 6. activation of modems for vendors only when needed by vendors, with immediate deactivation after use; and 7. prohibition of storage of covered data onto local hard drives, floppy disks, or other external media. Management: 1. clearly identifies applications, application stores and application extensions and plugins approved for bring your own device (BYOD) usage; 2. defines the device and eligibility requirements to allow for BYOD usage; 3. clarifies its expectations of privacy and its requirements for litigation, e-discovery, and legal holds with respect to mobile devices; 4. clearly states expectations regarding the loss of non-company data in the case a wipe of a mobile device is required; and 5. clarifies the systems and servers allowed for use or access on a BYOD-enabled device.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 PL-04 (HIGH; MOD) CMSRs v3.1 PM-02 (HIGH; MOD) CSA CCM v3.0.1 MOS-04 CSA CCM v3.0.1 MOS-06 CSA CCM v3.0.1 MOS-08 CSA CCM v3.0.1 MOS-13 CSA CCM v3.0.1 MOS-20 FedRAMP PL-4 FFIEC IS v2016 A.2.7 FFIEC IS v2016 A.2.9 IRS Pub 1075 v2016 9.3.12.3 IRS Pub 1075 v2016 9.3.12.3.1 IRS Pub 1075 v2016 9.3.12.3.2 IRS Pub 1075 v2016 9.3.12.3.6 IRS Pub 1075 v2016 9.3.12.3.7 IRS Pub 1075 v2016 9.3.18.1 ISO/IEC 27002:2013 7.2.1 ISO/IEC 27799:2016 7.2.1 MARS-E v2 PL-4 MARS-E v2 PM-2 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 PR.AT-1 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 AC-20(3)[S]{1} NRS 603A.215.1

	PCI DSS v3.2.1 12.3.5 PMI DSP Framework PR.AC-1

Level DGF Implementation Requirements

Level DGF Implementation:	Operational processes for Data Governance have been implemented and integrated into work. Data Custodians ensure that the strategic vision for Data Governance satisfies short-, mid-, and long-term needs of the custodian's domain/application/business segment, as applicable.

Control Reference: 02.e Information Security Awareness, Education, and Training

Control Specification:	All employees of the organization, and contractors and third-party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Awareness and Training; IT Organization and Management Roles and Responsibilities; Personnel; Policies and Procedures

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 2 Subject to HIPAA Security Rule Subject to NIST 800-171 Basic Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to State of Massachusetts Data Protection Act Subject to Texas Health and Safety Code
Level 1 Implementation:	Awareness training commences with a formal induction process designed to introduce the organization's security and privacy policies, state and federal laws, and expectations before access to information or services is granted and no later than 60 days after the date the employee, contractor, and other workforce member is hired, or a contractual arrangement is made with a collaborating organization. At a minimum, the organizations security awareness and training program will identify how workforce members are provided security awareness and training; identify the workforce members (including managers, senior executives, and as appropriate, business associates/partners, and contractors) who will receive security awareness and training; describe the types of security awareness and training that is reasonable and appropriate for its workforce members; how workforce members are provided security and awareness training when there is a change in the organizations information

	systems; and how frequently security awareness and training is provided to all workforce members. Ongoing training for these individuals and organizations includes security and privacy requirements (e.g., objective, scope, roles and responsibilities, coordination, compliance, communicating threat information, legal responsibilities, and business controls) as well as training in the correct use of information assets and facilities (including, but not limited to, log-on procedures, use of software packages, anti-malware for mobile devices, and information on the disciplinary process. Training discusses how the organization addresses each area (e.g., audit logging and monitoring); how events or incidents are identified (e.g., monitoring for inappropriate or failed user logins), and the actions the organization takes in response to events or incidents (e.g., notifying the workforce member or the members supervisor), as appropriate to the area of training. The organization provides incident response and contingency training to information system users consistent with assigned roles and responsibilities: 1. within 90 days of assuming an incident response role or responsibility; 2. when required by information system changes; and 3. within every 365 days thereafter. The organization documents that the training has been provided to the individual. A list of applications, application stores, and application extensions and plugins approved for bring your own device (BYOD) usage is provided during training.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 201 CMR 17.04(8) 45 CFR Part § 164.308(a)(5)(i) HIPAA.SR-2 45 CFR Part § 164.308(a)(5)(ii)(A) HIPAA.SR-1 45 CFR Part § 164.530(b)(1) HIPAA.PR 45 CFR Part § 164.530(b)(2) HIPAA.PR AICPA 2017 CC1.1 AICPA 2017 CC2.2 AICPA 2017 CC2.3 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CIS CSC v7.1 17.3 CMMC v1.0 AT.2.056-0 CMSRs v3.1 AR-05 (HIGH; MOD) CMSRs v3.1 AT-01 (HIGH; MOD) CMSRs v3.1 AT-02 (HIGH; MOD) CMSRs v3.1 AT-03 (HIGH; MOD) CMSRs v3.1 CP-03 (HIGH; MOD) CMSRs v3.1 CP-03(01) (HIGH; MOD) CMSRs v3.1 CP-04 (HIGH) CMSRs v3.1 IR-02 (HIGH; MOD) CMSRs v3.1 PM-14 (HIGH; MOD) CRR v2016 SA:G3.Q3 CRR v2016 TA:G1.Q1 CRR v2016 TA:G1.Q4 CRR v2016 TA:G2.Q7 CRR v2016 TA:MIL2.Q4 CSA CCM v3.0.1 HRS-09 CSA CCM v3.0.1 MOS-01 CSA CCM v3.0.1 MOS-04 CSA CCM v3.0.1 MOS-05 De-ID Framework v1 Privacy and Security Training: General FedRAMP AT-1 FedRAMP AT-2 FedRAMP AT-3 FedRAMP CP-4 FedRAMP IR-2 FFIEC IS v2016 A.6.8(f) IRS Pub 1075 v2016 9.3.2.1 IRS Pub 1075 v2016 9.3.2.2 IRS Pub 1075 v2016 9.3.2.3 IRS Pub 1075 v2016 9.3.6.3

	IRS Pub 1075 v2016 9.3.8.2 ISO/IEC 27002:2013 7.2.2 ISO/IEC 27799:2016 7.2.2 MARS-E v2 AR-5 MARS-E v2 AT-1 MARS-E v2 AT-2 MARS-E v2 AT-3 MARS-E v2 CP-3 MARS-E v2 CP-4 MARS-E v2 IR-2 NIST 800-171 r2 3.2.1-0 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 PR.AT-1 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 AT-2[HML]{0} NIST SP 800-53 R4 AT-3(3)[S]{1} NIST SP 800-53 R4 CP-3[HML]{0} NIST SP 800-53 R4 IR-2[HML]{0} NIST SP 800-53 R4 IR-8e[HML]{0} NIST SP 800-53 R4 PM-13[HML]{0} NY DOH SSP v3.1 AT-2[M]-0 NY DOH SSP v3.1 AT-2b[M]-0 NY DOH SSP v3.1 AT-2c[M]-0 NY DOH SSP v3.1 AT-3[M]-0 NY DOH SSP v3.1 AT-3c[M]-1 NY DOH SSP v3.1 AT-4b[M]-1 NY DOH SSP v3.1 CP-3[M]-0 NY DOH SSP v3.1 CP-3a[M]-0 NY DOH SSP v3.1 CP-3b[M]-0 NY DOH SSP v3.1 CP-3c[M]-0 PMI DSP Framework PR.AT-2

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to 23 NYCRR 500 Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 3 Subject to CMMC Level 4 Subject to EHNAC Accreditation Subject to FTC Red Flags Rule Subject to HIPAA Security Rule Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to Texas Health and Safety Code
Level 2 Implementation:	Level 1 plus:

	The organization formally creates dedicated security awareness training as part of a resource on-boarding process to the organization. The organization documents its formal induction security awareness training process. The organization conducts an internal annual review of the effectiveness of its security and privacy education and training program and updates the program to reflect risks identified in the organizations risk assessment. The organization manages a security and privacy education and training program for all employees and contractors with tracking of completion and a requirement for refresher training at least every 365 days. Employees are required to acknowledge they have received training and are aware of their responsibilities through signoff. The organization includes security awareness training on recognizing and reporting potential indicators of an insider threat. The organization's security personnel, including organizational business unit security points of contact, receive specialized security education and training appropriate to their role/responsibilities. Train developers at least annually in up-to-date, secure coding techniques, including how to avoid common coding vulnerabilities. Ensure developers understand how sensitive data is handled in memory. The organization's awareness program: 1. focuses on the methods commonly used in intrusions that can be blocked through individual action; 2. delivers content in short online modules convenient for employees; 3. receives frequent updates (at least annually) to address the latest attack techniques; and 4. includes the senior leadership teams personal messaging and involvement. The organization trains its workforce to ensure covered information is stored in organization-specified locations. The organization ensures that the senior executives have been trained in their specific roles and responsibilities.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(3) 1 TAC § 390.2(a)(4)(A)(xi) 16 CFR Part § 681.1 (e)(3) 23 NYCRR 500.14(b) 45 CFR Part § 164.308(a)(5)(i) HIPAA.SR-1 45 CFR Part § 164.530(b)(1) HIPAA.PR 45 CFR Part § 164.530(b)(2) HIPAA.PR AICPA 2017 CC1.1 AICPA 2017 CC1.4 AICPA 2017 CC2.3 CIS CSC v7.1 17.3 CIS CSC v7.1 18.6 CMMC v1.0 AT.3.058-0 CMMC v1.0 AT.4.059-2 CMSRs v3.1 AR-05 (HIGH; MOD) CMSRs v3.1 AT-02 (HIGH; MOD) CMSRs v3.1 AT-02(02) (HIGH; MOD) CMSRs v3.1 AT-03 (HIGH; MOD) CMSRs v3.1 IR-02(01) (HIGH) CMSRs v3.1 IR-02(02) (HIGH) CMSRs v3.1 PL-04 (HIGH; MOD) CMSRs v3.1 PL-4 (HIGH; MOD) CMSRs v3.1 PM-06 (HIGH; MOD) CMSRs v3.1 PM-14 (HIGH; MOD) CRR v2016 TA:G1.Q2 CRR v2016 TA:G2.Q1 CRR v2016 TA:G2.Q2 CRR v2016 TA:G2.Q3 CRR v2016 TA:G2.Q4 CRR v2016 TA:G2.Q5 CRR v2016 TA:G2.Q6

	CRR v2016 TA:G2.Q7 CRR v2016 TA:MIL2.Q1 CRR v2016 TA:MIL2.Q4 CRR v2016 TA:MIL4.Q1 CSA CCM v3.0.1 HRS-09 De-ID Framework v1 Storage (Minimal Locations Authorized): Implementation FedRAMP AT-2 FedRAMP AT-2(2) FedRAMP AT-3 FedRAMP PL-4 FFIEC IS v2016 A.6.8(f) IRS Pub 1075 v2016 9.3.12.3 IRS Pub 1075 v2016 9.3.2.2 IRS Pub 1075 v2016 9.3.2.3 ISO/IEC 27002:2013 7.2.2 ISO/IEC 27799:2016 7.2.2 MARS-E v2 AR-5 MARS-E v2 AT-2 MARS-E v2 AT-2(2) MARS-E v2 AT-3 MARS-E v2 PL-4 MARS-E v2 PM-14 MARS-E v2 PM-6 NIST 800-171 r2 3.2.3-0 NIST Cybersecurity Framework v1.1 PR.AT-1 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 AT-2(2)[HM]{0} NIST SP 800-53 R4 AT-4a[HML]{0} NIST SP 800-53 R4 PL-4b[HML]{1} NRS 603A.215.1 NY DOH SSP v3.1 AT-2(2).IS1[HML]-0 NY DOH SSP v3.1 AT-4b[M]-2 NY DOH SSP v3.1 PM-14.PII[M]-1 PCI DSS v3.2.1 12.6 PCI DSS v3.2.1 12.6.1 PCI DSS v3.2.1 12.6.2 PCI DSS v3.2.1 6.5 PCI DSS v3.2.1 9.9 PCI DSS v3.2.1 9.9.3 PMI DSP Framework PR.AT-2

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to Banking Requirements Subject to CMMC Level 2 Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Basic Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate)

	Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Texas Health and Safety Code Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: Personnel with significant information security roles and responsibilities are required to undergo appropriate role-based information system security training: 1. prior to authorizing access to the organization's networks, systems, and/or applications; 2. when required by significant information system or system environment changes; 3. when an employee enters a new position that requires additional role-specific training; and 4. refresher training annually thereafter. The organization maintains a documented list of each individual who completes the on-boarding process. Training records are retained for at least five years thereafter. Workforce members are trained on how to properly respond to perimeter security alarms (see 08.b, level 3).
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMMC v1.0 AT.2.057-0 CMSRs v3.1 AT-03 (HIGH; MOD) CMSRs v3.1 AT-04 (HIGH; MOD) CMSRs v3.1 IR-02 (HIGH; MOD) CMSRs v3.1 SA-16 (HIGH) CRR v2016 TA:G1.Q2 CRR v2016 TA:G2.Q5 De-ID Framework v1 Perimeter Security (Alarms): Testing FedRAMP AT-3 FedRAMP AT-4 IRS Pub 1075 v2016 9.3.2.3 IRS Pub 1075 v2016 9.3.2.4 IRS Pub 1075 v2016 9.3.8.2 IRS Pub 1075 v2016 Exhibit 10 MARS-E v2 AT-3 MARS-E v2 AT-4 MARS-E v2 IR-2 NIST 800-171 r2 3.2.2-0 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 PR.AT-2 NIST Cybersecurity Framework v1.1 PR.AT-5 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 AT-3[HML]{0} NIST SP 800-53 R4 AT-4b[HML]{0} NIST SP 800-53 R4 SA-19(1)[S]{0} NY DOH SSP v3.1 AT-3a[M]-0 NY DOH SSP v3.1 AT-3b[M]-0 NY DOH SSP v3.1 AT-3c[M]-2 NY DOH SSP v3.1 AT-4c[M]-0

Level CIS Implementation Requirements

Level CIS Implementation:	The organization performs a gap analysis to see which skills employees need and which behaviors employees are not adhering to, uses this information to build a baseline training and awareness roadmap for all employees, and delivers additional awareness and training content to fill the skills gaps through an awareness and training program.

Level CMS Implementation Requirements

Level CMS Implementation:	The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations. The organization employs automated mechanisms to provide a more thorough and realistic training environment. The organization requires the developer of the information system, system component, or information system service to provide appropriate training (or training materials), for affected personnel, on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

Level DGF Implementation Requirements

Level DGF Implementation:	Individuals are adequately trained on the Data Governance framework, policies, and related implementation expectations.

Level EHNAC Implementation Requirements

Level EHNAC Implementation:	Awareness training includes training on the organization's breach reporting policies and procedures.

Level Federal Implementation Requirements

Level Federal Implementation:	The organization establishes and implements an Operations Security (OPSEC) program.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The organization provides contingency training to information system users consistent with assigned roles and responsibilities within 10 days of assuming an incident response role or responsibility, when required by information system changes, and within every 365 days thereafter.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	Awareness training specific to protecting and disclosing FTI, including how FTI security requirements are communicated to end users, and the (possible) sanctions for misuse of FTI must be provided initially prior to granting access to FTI and annually thereafter. The disclosure awareness (training) requirements apply to all agency employees with access to FTI, including program and information technology personnel and contractors, such as case workers, managers, system administrators, database administrators and application developers. Training is user specific to ensure that all personnel receive appropriate training for a particular job, such as training required for administrators or auditors. Granting employees or contractors access to FTI must be preceded by each employee or contractor certifying his/her understanding of the agency's security policy and procedures for safeguarding FTI. The certification must be maintained for five years. The organization provides refresher training, prior to access of FTI and annually thereafter, on incident response policy and procedure regarding FTI.

	The agency must provide contingency and incident response training to information system users consistent with assigned roles and responsibilities prior to assuming a contingency role or responsibility.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The organization provides incident response training to information system users consistent with assigned roles and responsibilities: (i) within one [1] month of assuming an incident response role or responsibility; (ii) when required by information system changes; and (iii) within every 365 days thereafter. The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users, prior to accessing any system's information. An information security and privacy education and awareness training program must be developed and implemented for all employees and individuals working on behalf of CMS who access, use, manage, or develop information systems. Information security and privacy education and awareness training must address individuals' responsibilities associated with sending sensitive information in email. Privacy awareness training must be provided before granting access to CMS systems and networks, and within every [365] days thereafter, to all employees and contractors, to explain the importance of and responsibility for safeguarding PII and ensuring privacy, as established in federal legislation and OMB guidance. Provide privacy training for all systems that collect, maintain, store, use, or disclose PII, commensurate with the PII confidentiality impact level. Integrate privacy training with general Information Assurance training. The organization includes security awareness and training on recognizing and reporting potential indicators of insider threats, such as (i) inordinate, long-term job dissatisfaction, (ii) attempts to gain access to information not required for job performance, (iii) unexplained access to financial resources, (iv) bullying or sexual harassment of fellow employees, (v) workplace violence, and (vi) other serious violations of organizational policies, procedures, directives, rules, or practices. All CMS employees and contractors with significant information security roles and responsibilities that have not completed the required training within the mandated timeframes shall have their user accounts disabled until they have met their RBT requirement. The organization provides training to its personnel on organization-defined indicators of malicious code to recognize suspicious communications and anomalous behavior in organizational information systems.

Level PCI Implementation Requirements

Level PCI Implementation:	The organization ensures that all personnel are aware of the cardholder data security policy and procedures as part of the formal security awareness program. The organization trains personnel to be aware of attempted tampering or replacement of devices. Training includes the following: 1. Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.

	2. Do not install, replace, or return devices without verification. 3. Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). 4. Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).

Level Title 21 CFR Part 11 Implementation Requirements

Level Title 21 CFR Part 11 Implementation:	Persons who develop, maintain, or use electronic record/electronic signature systems must have the proper and sufficient education, training, and experience to perform their assigned tasks.

Control Reference: 02.f Disciplinary Process

Control Specification:	There shall be a formal disciplinary process for employees who have violated security policies and procedures. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Documentation and Records; Incident Response; IT Organization and Management Roles and Responsibilities; Personnel; Policies and Procedures; Requirements (Legal and Contractual)

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to HIPAA Security Rule Subject to HITRUST De-ID Framework Requirements Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to State of Massachusetts Data Protection Act Subject to Texas Health and Safety Code Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures and notifies defined personnel (e.g., supervisors) within a defined time frame (e.g., 24 hours) when a formal sanction process is initiated, identifying the individual sanctioned and the reason for the sanction. The disciplinary process is not commenced without prior verification that a security breach has occurred. The formal disciplinary process ensures correct and fair treatment for employees who are suspected of committing breaches of security. The formal disciplinary process provides for a graduated response that takes into consideration factors such as the nature and gravity of the breach and its impact on business, whether or not this is a first or repeat offense, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required. And for each incident, the organization documents the personnel involved in the disciplinary process, the steps taken, and the timeline associated with those steps, the steps taken for

	notification, the rationale for the discipline, whether the discipline was due to a compliance failure, and the final outcome. The organization includes specific procedures for license, registration, and certification denial or revocation and other disciplinary action. The organization maintains a list or documents an indication of employees involved in security incident investigations and the resulting outcome in their HR folder. The organization ensures individuals are held accountable and responsible for actions initiated under their electronic signatures, to help deter record and signature falsification.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 1 TAC § 390.2(a)(4)(B)(xviii)(I) 1 TAC § 390.2(a)(4)(B)(xviii)(II) 1 TAC § 390.2(a)(4)(B)(xviii)(III) 201 CMR 17.03(2)(d) 21 CFR Part 11.10(j) 45 CFR Part § 164.308(a)(1)(ii)(C) HIPAA.SR-0 45 CFR Part § 164.530(e) HIPAA.PR AICPA 2017 CC1.1 AICPA 2017 CC1.5 AICPA 2017 CC5.3 AICPA 2017 CC7.4 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 IR-05 (HIGH; MOD) CMSRs v3.1 PS-08 (HIGH; MOD) CSA CCM v3.0.1 GRM-07 De-ID Framework v1 Sanctions: General FedRAMP IR-5 FedRAMP PS-8 HITRUST IRS Pub 1075 v2016 9.3.13.8 IRS Pub 1075 v2016 9.3.8.5 ISO/IEC 27002:2013 7.2.3 ISO/IEC 27799:2016 7.2.3 MARS-E v2 IR-5 MARS-E v2 PS-8 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 PS-8[HML]{0} NY DOH SSP v3.1 PS-8a[M]-0 NY DOH SSP v3.1 PS-8b[M]-0 OCR Audit Protocol (2016) 164.308(a)(1)(ii)(C)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to the CMS Minimum Security Requirements (High)

Level 2 Implementation:	Level 1 plus: The organization creates a point of contact from HR to handle any incidents relating to employees. The organization notifies the CISO or a designated representative of the application of a formal employee sanctions process, identifying the individual and the reason for the sanction.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.530(e)(1) HIPAA.PR 45 CFR Part § 164.530(e)(2) HIPAA.PR CMSRs v3.1 PS-08 (HIGH) CSA CCM v3.0.1 GRM-07 FedRAMP PS-8 HITRUST IRS Pub 1075 v2016 9.3.13.8 ISO/IEC 27002:2013 7.2.3 ISO/IEC 27799:2016 7.2.3 MARS-E v2 PS-8 NIST Cybersecurity Framework v1.1 PR.IP-11

Level EHNAC Implementation Requirements

Level EHNAC Implementation:	The organization's formal sanctions process includes failure to comply with established privacy policies and procedures.

Objective Name: 02.04 Termination or Change of Employment

Control Objective:	To ensure that the access rights are properly removed and that assets are recovered for employees and contractors who have been terminated or transferred.

Control Reference: 02.g Termination or Change Responsibilities

Control Specification:	Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.
Factor Type:	Organizational
Topics:	Awareness and Training; IT Organization and Management Roles and Responsibilities; Personnel; Requirements (Legal and Contractual); Third-parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 2 Subject to HIPAA Security Rule Subject to NIST 800-171 Basic Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental)

	Subject to NY OHIP Moderate-Plus Security Baseline Subject to Texas Health and Safety Code
Level 1 Implementation:	Logical and physical access authorizations to systems and equipment are reviewed, updated, or revoked when there is any change in responsibility or employment. The organization formally addresses: 1. terminating access when the access is no longer needed; 2. assignment of responsibility for removing information system and/or physical access; and 3. timely communication of termination actions to ensure that the termination procedures are appropriately followed (see 02.i). When an employee or other workforce member moves to a new position of trust, logical and physical access controls must be re-evaluated as soon as possible but not to exceed 30 days. The organization also ensures employees or workforce members that are terminated understand their obligations to ensure any covered information for which they had prior access remains confidential (e.g., during an exit interview).
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.308(a)(3)(ii)(C) HIPAA.SR-0 AICPA 2017 CC6.4 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CIS CSC v7.1 16.7 CMMC v1.0 PS.2.128-0 CMSRs v3.1 PS-04 (HIGH; MOD) CMSRs v3.1 PS-05 (HIGH; MOD) CSA CCM v3.0.1 HRS-04 CSA CCM v3.0.1 IAM-11 FedRAMP PS-4 FedRAMP PS-5 FFIEC IS v2016 A.6.8(c) HITRUST IRS Pub 1075 v2016 9.3.13.4 IRS Pub 1075 v2016 9.3.13.5 ISO/IEC 27002:2013 6.1.1 ISO/IEC 27002:2013 7.3.1 ISO/IEC 27002:2013 9.2.5 ISO/IEC 27002:2013 9.2.6 ISO/IEC 27799:2016 6.1.1 ISO/IEC 27799:2016 7.3.1 ISO/IEC 27799:2016 9.2.6 MARS-E v2 PS-4 MARS-E v2 PS-5 NIST 800-171 r2 3.9.2-0 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 PS-4(1)b[S]{2} NIST SP 800-53 R4 PS-4a[HML]{1} NIST SP 800-53 R4 PS-4b[HML]{0} NIST SP 800-53 R4 PS-5a[HML]{0} NIST SP 800-53 R4 PS-5b[HML]{0} NY DOH SSP v3.1 AC-2b[M]-1 NY DOH SSP v3.1 PS-4b[M]-1 NY DOH SSP v3.1 PS-4b[M]-2 NY DOH SSP v3.1 PS-4c[M]-0 NY DOH SSP v3.1 PS-5a[M]-0 NY DOH SSP v3.1 PS-5b4[M]-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives

	HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The organization has a documented termination process for all employees and other workforce members. The organization has a process where exit interviews address organization-defined information and security items, all organization information-system-related property and access is retrieved and revoked, knowledge transfer/information transitioned, and provides appropriate personnel with access to official records created by a terminated employee or when the arrangement of a workforce member ends. The organization defines any valid duties after termination of employment or when the arrangement of a workforce member ends and is included in the employee's or workforce member's contract or other arrangement. The communication of termination responsibilities includes ongoing security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement and the terms and conditions of employment or other workforce arrangement continuing for a defined period after the end of the employee's, contractor's or third-party user's employment or other workforce arrangement.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 PS-04 (HIGH; MOD) FedRAMP PS-4 IRS Pub 1075 v2016 9.3.13.4 ISO/IEC 27002:2013 7.3.1 ISO/IEC 27799:2016 7.3.1 MARS-E v2 PS-4 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 PS-4(1)a[S]{0} NIST SP 800-53 R4 PS-4c[HML]{0} NIST SP 800-53 R4 PS-4d[HML]{0} NIST SP 800-53 R4 PS-4e[HML]{0} NY DOH SSP v3.1 PS-4d[M]-2 NY DOH SSP v3.1 PS-4e[M]-0

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB)

	Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to FedRAMP Certification
Level 3 Implementation:	Level 2 plus: The organization has a documented termination checklist that identifies all the steps to be taken and assets collected.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 PS-04 (HIGH; MOD) FedRAMP PS-4 HITRUST IRS Pub 1075 v2016 9.3.13.4 MARS-E v2 PS-4 NIST Cybersecurity Framework v1.1 PR.IP-11

Level CMS Implementation Requirements

Level CMS Implementation:	All access and privileges to CMS systems, networks, and facilities are suspended when employees or contractors temporarily separate from the organization (e.g., leave of absence). The organization: 1. Initiates the following transfer or reassignment actions during the formal transfer process: i. re-issuing appropriate information system-related property (e.g., keys, identification cards, building passes); ii. notification to security management; iii. closing obsolete accounts and establishing new accounts; and 2. notifies defined personnel or roles (defined in the applicable security plan) within one business day.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	When personnel are transferred or reassigned, the organization notifies defined personnel or roles within five business days.

Control Reference: 02.h Return of Assets

Control Specification:	All employees, contractors, and third-party users shall return all of the organization's assets in their possession upon termination of their employment, contract, or agreement.
Factor Type:	Organizational
Topics:	Media and Assets; Personnel; Third-parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations

Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NY OHIP Moderate-Plus Security Baseline Subject to State of Massachusetts Data Protection Act Subject to Texas Health and Safety Code Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	The termination process includes the return of all previously issued software, corporate documents, and equipment. Other organizational assets such as mobile computing devices, credit cards, access cards, manuals, and information stored on electronic media are also returned. In cases where an employee, contractor or third-party user purchases the organization's equipment or uses their own personal equipment, procedures are followed to ensure that all relevant information is transferred to the organization and securely erased from the equipment. In cases where an employee, contractor or third-party user has knowledge that is important to ongoing operations, that information is documented and transferred to the organization.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 201 CMR 17.03(2)(e) CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 PS-04 (HIGH; MOD) CSA CCM v3.0.1 HRS-01 FedRAMP PS-4 IRS Pub 1075 v2016 9.3.13.4 ISO/IEC 27002:2013 8.1.4 ISO/IEC 27799:2016 8.1.4 MARS-E v2 PS-4 NIST Cybersecurity Framework v1.1 PR.IP-11 NY DOH SSP v3.1 PS-4d[M]-1

Control Reference: 02.i Removal of Access Rights

Control Specification:	The access rights of all employees, contractors, and third-party users to information and information assets shall be removed upon termination of their employment, contract, or agreement, or adjusted upon a change of employment (i.e., upon transfer within the organization). *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Authorization; Personnel; Third-parties and Contractors; User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 1 Subject to FISMA Compliance Subject to NIST 800-171 Derived Level

	Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to State of Massachusetts Data Protection Act Subject to Supplemental Requirements Subject to Texas Health and Safety Code
Level 1 Implementation:	Upon termination, the access rights for the terminated individual are disabled in a timely manner, at least within 24 hours. Changes of employment or other workforce arrangement (e.g., transfers) are reflected in removal of all access rights that were not approved for the new employment or workforce arrangement. Access changes due to personnel transfer are managed effectively. Old accounts are closed after 90 days, and new accounts opened. The access rights that are removed or adapted include physical and logical access, keys, identification cards, IT systems and applications, subscriptions, and removal from any documentation that identifies them as a current member of the organization. If a departing employee, contractor, third-party user, or other workforce member has known passwords for accounts remaining active, these are changed upon termination or change of employment, contract, agreement, or other workforce arrangement. Access rights to information assets and facilities are reduced or removed before the employment or other workforce arrangement terminates or changes, depending on the evaluation of risk factors including: 1. whether the termination or change is initiated by the employee, contractor, third-party user, other workforce member, or by management, and the reason for termination; 2. the current responsibilities of the employee, contractor, workforce member, or any other user; and 3. the value of the assets currently accessible.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMMC v1.0 PE.1.134-1 CMSRs v3.1 AC-2 (HIGH; MOD) CMSRs v3.1 PS-05 (HIGH; MOD) CSA CCM v3.0.1 IAM-11 FedRAMP AC-2 FedRAMP PS-5 IRS Pub 1075 v2016 9.3.1.2 IRS Pub 1075 v2016 9.3.13.4 IRS Pub 1075 v2016 9.3.13.5 ISO/IEC 27002:2013 9.2.6 ISO/IEC 27799:2016 9.2.6 MARS-E v2 AC-2 MARS-E v2 PS-5 NIST 800-171 r2 3.10.5-1 NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 PE-3g[HML]{1} NIST SP 800-53 R4 PS-5c[HML]{0} NRS 603A.215.1 NY DOH SSP v3.1 PS-4.IS1[HM]-0 NY DOH SSP v3.1 PS-4a[M]-1 NY DOH SSP v3.1 PS-4a[M]-2 PCI DSS v3.2.1 8.1.3 SR v6.4 19b-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to FedRAMP Certification Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The organization employs automated mechanisms to notify specific personnel or roles (formally defined by the organization) upon termination of an individual. Organizations immediately terminate the access rights following the supply of a resignation notice, notice of dismissal, etc., prior to or during the personnel termination process. Termination allows for immediate escorting out of the site, if necessary, wherever continued access is perceived to cause an increased risk, e.g., in the case of serious misconduct.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 PS-04 (HIGH; MOD) CMSRs v3.1 PS-04(02) (HIGH) FedRAMP PS-4 IRS Pub 1075 v2016 9.3.13.4 ISO/IEC 27002:2013 9.2.6 ISO/IEC 27799:2016 9.2.6 MARS-E v2 PS-4 NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 PS-4(2)[H]{0} NIST SP 800-53 R4 PS-4a[HML]{2} NRS 603A.215.1 NY DOH SSP v3.1 PS-4(2).IS1[H]-1 NY DOH SSP v3.1 PS-4(2)[HN]-0 NY DOH SSP v3.1 PS-4f[M]-1 NY DOH SSP v3.1 PS-4g[M]-0 PCI DSS v3.2.1 8.1.3

Level Providers Implementation Requirements

Level Providers Implementation:	All organizations that process protected health information, as soon as possible, terminate the user access privileges with respect to such information for any departing permanent or temporary employee, third-party contractor, or volunteer upon termination of employment, contracting, or volunteer activities.

Control Category: 03.0 - Risk Management

Objective Name: 03.01 Risk Management Program

Control Objective:	To develop and implement a Risk Management Program that addresses Risk Assessments, Risk Mitigation, and Risk Evaluations.

Control Reference: 03.a Risk Management Program Development

Control Specification:	Organizations shall develop and maintain a risk management program to manage risk to an acceptable level.
Factor Type:	Organizational
Topics:	Policies and Procedures; Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to HITRUST De-ID Framework Requirements Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Privacy) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Texas Health and Safety Code Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	The organization: 1. develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, and other organizations associated with the operation and use of information systems, including physical and environmental hazards; 2. implements the strategy consistently across the organization, and 3. ensures that their information protection programs do not apply safeguards unnecessarily, e.g., to de-identified information. Elements of the risk management program include: 1. the creation of a risk management policy for information systems and paper records that is formally approved by management and includes: i. objectives of the risk management process; ii. management's clearly stated level of acceptable risk, informed by its role in the critical infrastructure and business-specific risk analysis; iii. the connection between the risk management policy and the organization's strategic planning processes; and iv. documented risk assessment processes and procedures. 2. regular performance of risk assessments;

	3. mitigation of risks identified from risk assessments and threat monitoring procedures; 4. risk tolerance thresholds are defined for each category of risk; 5. the plan for managing operational risk communicated to stakeholders; 6. reassessment of the risk management policy to ensure management's stated level of acceptable risk is still accurate, previously decided upon security controls are still applicable and effective, and to evaluate the possible risk-level changes in the environment; 7. updating the risk management policy if any of these elements have changed; and 8. repeating the risk management process prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, or at a minimum annually.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 1 TAC § 390.2(b) AICPA 2017 CC3.3 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 AR-02 (HIGH; MOD) CMSRs v3.1 PM-09 (HIGH; MOD) CMSRs v3.1 PM-11 (HIGH; MOD) CMSRs v3.1 RA-01 (HIGH; MOD) CMSRs v3.1 RA-03 (HIGH; MOD) CRR v2016 AM:MIL3.Q4 CRR v2016 CM:G1.Q2 CRR v2016 CM:MIL2.Q4 CRR v2016 CM:MIL3.Q4 CRR v2016 EDM:MIL2.Q2 CRR v2016 EDM:MIL3.Q4 CRR v2016 IM:MIL3.Q4 CRR v2016 RM:G1.Q1 CRR v2016 RM:G1.Q2 CRR v2016 RM:G1.Q3 CRR v2016 RM:G1.Q4 CRR v2016 RM:G2.Q3 CRR v2016 RM:G2.Q4 CRR v2016 RM:G3.Q1 CRR v2016 RM:G5.Q1 CRR v2016 RM:MIL2.Q4 CRR v2016 RM:MIL3.Q4 CRR v2016 RM:MIL4.Q3 CRR v2016 SA:G1.Q2 CRR v2016 SA:MIL2.Q1 CRR v2016 SA:MIL2.Q4 CRR v2016 SA:MIL3.Q4 CRR v2016 TA:MIL3.Q4 CRR v2016 VM:MIL2.Q1 CSA CCM v3.0.1 GRM-11 EU GDPR Article 32(2) FedRAMP RA-1 FedRAMP RA-3 FFIEC IS v2016 A.2.11 FFIEC IS v2016 A.3.1 FFIEC IS v2016 A.6.4(a) FFIEC IS v2016 A.7.1 FFIEC IS v2016 A.7.2 FFIEC IS v2016 A.7.3 IRS Pub 1075 v2016 9.3.14.1 IRS Pub 1075 v2016 9.3.14.2 MARS-E v2 AR-2 MARS-E v2 PM-11 MARS-E v2 PM-9 MARS-E v2 RA-1 MARS-E v2 RA-3 NIST Cybersecurity Framework v1.1 ID.BE-3 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 ID.RM-1 NIST Cybersecurity Framework v1.1 ID.RM-2 NIST Cybersecurity Framework v1.1 ID.RM-3 NIST Cybersecurity Framework v1.1 ID.SC-2

	NIST Cybersecurity Framework v1.1 RS.MI-3 NIST SP 800-53 R4 DI-1[P]{0} NIST SP 800-53 R4 DM-1[P]{0} NIST SP 800-53 R4 PM-9a[HML]{0} NIST SP 800-53 R4 PM-9c[HML]{0} NY DOH SSP v3.1 PM-9a[M]-0 NY DOH SSP v3.1 PM-9c[M]-2 PMI DSP Framework ID-1 PMI DSP Framework ID-2

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CRR V2016 Subject to FedRAMP Certification Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate)
Level 2 Implementation:	Level 1 plus: Formal risk assessment and risk treatment processes are implemented, including a repository and tracking system for risk assessments performed, and risk mitigation is completed or underway.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 PM-04 (HIGH; MOD) CMSRs v3.1 RA-01 (HIGH; MOD) CRR v2016 RM:G5.Q2 CRR v2016 RM:MIL2.Q4 CRR v2016 RM:MIL3.Q4 CRR v2016 VM:G2.Q6 CRR v2016 VM:MIL2.Q1 FedRAMP RA-1 FFIEC IS v2016 A.2.11 FFIEC IS v2016 A.3.1 FFIEC IS v2016 A.7.1 FFIEC IS v2016 A.7.2 FFIEC IS v2016 A.7.3 IRS Pub 1075 v2016 9.3.14.1 MARS-E v2 PM-4 MARS-E v2 RA-1 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST SP 800-53 R4 PM-9b[HML]{0}

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB)

	Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to FTC Red Flags Rule Subject to Texas Health and Safety Code
Level 3 Implementation:	Level 2 plus: The organization develops and implements a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of an account or any existing account that involves, or is designed to permit, multiple payments or transactions. The organization defines and incorporates existing policies and implement procedures to: 1. identify relevant patterns, practices, or specific activities that indicate the possible existence of identity theft for the accounts, and incorporate those patterns, practices, and activities into its program; 2. detect patterns, practices, and activities that have been incorporated into the program; 3. respond appropriately to any patterns, practices, and activities that are detected to prevent and mitigate identity theft; and 4. ensure the program and patterns, practices, and activities are updated at least annually, to reflect changes in risks to customers and to the safety and soundness of the organization. 'Personal identifying information' (PII) [also personally identifiable information] means information that alone or in conjunction with other information identifies an individual, including an individual's: 1. Name, Social Security number, date of birth, or government-issued identification number; 2. Mother's maiden name; 3. Unique biometric data, including the individual's fingerprint, voice print, and retina or iris image; 4. Unique electronic identification number, address, or routing code; and 5. Telecommunication access device. The organization's identity theft program includes protections for financial and medical identity theft, as applicable to the organization.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(3) 16 CFR Part § 681 Appendix A I 16 CFR Part § 681 Appendix A II 16 CFR Part § 681 Appendix A V 16 CFR Part § 681.1 (b)(3) 16 CFR Part § 681.1 (d)(1) 16 CFR Part § 681.1 (d)(2) 16 CFR Part § 681.1 (f) NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 ID.RM-1 PMI DSP Framework ID-1

Level Cloud Service Providers	Implementation Requirements

Level Cloud Service Providers Implementation:	Cloud service providers review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.

Level De-ID Data Environment	**Implementation Requirements**
Level De-ID Data Environment Implementation:	The organization: 1. documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and 2. conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

Level EHNAC	**Implementation Requirements**
Level EHNAC Implementation:	The organization must maintain a general analysis of most likely scenarios for breaches of PHI security.

Level Federal	**Implementation Requirements**
Level Federal Implementation:	The organization: 1. documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and 2. conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

Level GDPR	**Implementation Requirements**
Level GDPR Implementation:	Organizations specifically apply security and privacy controls to all personal data, which includes but is not limited to PII or PHI.

Level SCIDSA	**Implementation Requirements**
Level SCIDSA Implementation:	The licensee is required to identify reasonably foreseeable threats, assess the likelihood and possible damage from such threats, assess its policies, procedures, and systems to manage threats, and implement safeguards to manage identified threats.

Control Reference: 03.b Performing Risk Assessments

Control Specification:	Risk Assessments shall be performed to identify and quantify risks. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational

Topics:	Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 2 Subject to HIPAA Security Rule Subject to HITRUST De-ID Framework Requirements Subject to NIST 800-171 Basic Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to State of Massachusetts Data Protection Act Subject to Texas Health and Safety Code
Level 1 Implementation:	Risk assessments are performed that address all the major domains of the HITRUST CSF. Risk assessments are consistent and identify information security risks to the organization. The organization accounts for risks from sources including prior incidents experienced, changes in the environment (e.g., new methods of attack, new sources of attack, new vulnerabilities), and any supervisory guidance (e.g., third-party consultancy). They may be quantitative, semi- or quasi-quantitative, or qualitative but are consistent and comparable, so the prioritization of resources to manage risk can be performed. Risk assessments are to be performed at planned intervals, or when major changes occur in the environment, and the results reviewed annually.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 16 CFR Part § 681 Appendix A II(b) 201 CMR 17.03(2)(b) 45 CFR Part § 164.308(a)(1)(ii)(A) HIPAA.SR-0 AICPA 2017 CC4.1 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMMC v1.0 RM.2.141-0 CMSRs v3.1 RA-03 (HIGH; MOD) CRR v2016 CCM:MIL3.Q4 CRR v2016 RM:G5.Q1 CRR v2016 RM:MIL2.Q4 CRR v2016 VM:MIL3.Q4 CSA CCM v3.0.1 GRM-02 De-ID Framework v1 Risk Assessments: Assessments FedRAMP RA-3 FFIEC IS v2016 A.4.1 FFIEC IS v2016 A.6.28(c) FFIEC IS v2016 A.6.4(a) FFIEC IS v2016 A.7.1 FFIEC IS v2016 A.7.2 FFIEC IS v2016 A.7.3 FFIEC IS v2016 A.7.4(e) FFIEC IS v2016 A.8.1(i) HITRUST ISO/IEC 27002:2013 12.6.1 ISO/IEC 27002:2013 17.1.1 ISO/IEC 27799:2016 12.6.1 ISO/IEC 27799:2016 17.1.1 MARS-E v2 RA-3 NIST 800-171 r2 3.11.1-0 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 ID.RA-1 NIST Cybersecurity Framework v1.1 ID.RA-3 NIST Cybersecurity Framework v1.1 ID.RA-4 NIST Cybersecurity Framework v1.1 ID.RA-5

	NIST Cybersecurity Framework v1.1 ID.RM-1 NIST SP 800-53 R4 RA-3a[HML]{0} NIST SP 800-53 R4 RA-3c[HML]{0} NRS 603A.215.1 NY DOH SSP v3.1 PM-9b[M]-0 PCI DSS v3.2.1 12.2

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to FTC Red Flags Rule Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The organization updates the results of a comprehensive risk assessment every 2 years, or whenever there is a significant change to the information system or operational environment, assesses a subset of the security controls within every 365 days during continuous monitoring, and reviews the risk assessment results annually. The organization employs assessors or assessment teams with an organization-defined level of independence to conduct security control assessments and ensure impartiality of the results. These assessors accept the results of an assessment performed by another assessor when the assessment meets the same organization-defined level of independence. A formal, documented process is in place for identifying risks and performing risk assessments, including the criteria for the evaluation and categorization of risks, and communicating the results of the risk assessments to the affected parties, and to management. A repository and tracking system are in place to manage risk assessments performed. The likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits is included in the risk assessment process. The likelihood and impact associated with inherent and residual risk are determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).

	Information security risk assessments requires knowledge of the following: 1. external environment factors that could exacerbate or moderate any or all of the levels of the risk components described previously; 2. the types of accounts offered by the organization; 3. the methods the organization provides to open and access its accounts; 4. knowledge and experiences of incident histories and actual case impact scenarios; and 5. systems architectures.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(3) 1 TAC § 390.2(a)(4)(A)(xi) 16 CFR Part § 681.1 (c) 23 NYCRR 500.09(b)(1) AICPA 2017 CC3.4 CMSRs v3.1 CA-02 (HIGH; MOD) CMSRs v3.1 RA-03 (HIGH; MOD) CRR v2016 AM:MIL4.Q1 CRR v2016 AM:MIL4.Q2 CRR v2016 CCM:MIL4.Q1 CRR v2016 CCM:MIL4.Q2 CRR v2016 CM:MIL4.Q1 CRR v2016 CM:MIL4.Q2 CRR v2016 EDM:MIL4.Q1 CRR v2016 IM:MIL4.Q1 CRR v2016 IM:MIL4.Q2 CRR v2016 RM:MIL2.Q1 CRR v2016 RM:MIL4.Q1 CRR v2016 RM:MIL5.Q2 CRR v2016 SA:MIL4.Q1 CRR v2016 SCM:MIL4.Q1 CRR v2016 TA:MIL4.Q1 CRR v2016 VM:MIL4.Q1c CSA CCM v3.0.1 GRM-10 FedRAMP CA-2 FedRAMP RA-3 FFIEC IS v2016 A.4.1 FFIEC IS v2016 A.7.1 FFIEC IS v2016 A.7.2 FFIEC IS v2016 A.7.3 FFIEC IS v2016 A.8.1(i) IRS Pub 1075 v2016 9.3.14.2 IRS Pub 1075 v2016 9.3.4.2 IRS Pub 1075 v2016 9.4.1 MARS-E v2 CA-2 MARS-E v2 RA-3 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 ID.RA-1 NIST Cybersecurity Framework v1.1 ID.RA-4 NIST Cybersecurity Framework v1.1 ID.RA-5 NIST SP 800-53 R4 CA-2b[HML]{0} NIST SP 800-53 R4 RA-3b[HML]{0} NIST SP 800-53 R4 RA-3d[HML]{0} NIST SP 800-53 R4 RA-3e[HML]{0} PCI DSS v3.2.1 12.2

Level CMMC Implementation Requirements

Level CMMC Implementation:	The organization analyzes the effectiveness of security solutions at least annually to address anticipated risk to the system and to the organization based on current and accumulated threat intelligence.

Level CMS Implementation Requirements

Level CMS Implementation:	The organization documents the risk assessment results in the applicable security plan. The organization assesses the security controls in the information system within every 365 days to determine the extent to which the controls are implemented correctly,

	operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The annual security risk assessment requirement as mandated by OMB requires all controls attributable to a system or application to be assessed over a three-year period. To meet this requirement, a subset of the CMSRs is tested each year so that all security controls are tested during a three-year period. The Business Owner notifies the CMS CISO within 30 days whenever updates are made to system security authorization artifacts or significant role changes occur (e.g., Business Owner, System Developer/Maintainer, ISSO). The organization disseminates risk assessment results to affected stakeholders, Business Owners(s), and the CMS CISO. The organization employs assessors or assessment teams with a CMS CISO-defined level of independence to conduct security control assessments and ensure impartiality of the results.

Level DGF Implementation Requirements	
Level DGF Implementation:	A process is in place to identify key business/systems/IT organizations to have Data Governance implemented.

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation:	The organization accepts the results of an assessment of any FedRAMP Accredited 3PAO performed by any FedRAMP Accredited 3PAO when the assessment meets the conditions of an Authorizing Official in the FedRAMP Repository.

Level FFIEC IS Implementation Requirements	
Level FFIEC IS Implementation:	The organization implements a risk identification process that produces manageable groupings of information security threats, which include the following: 1. A threat assessment to help focus the risk identification efforts. 2. A method or taxonomy for categorizing threats, sources, and vulnerabilities. 3. A process to determine the institution's information security risk profile. 4. A validation of the risk identification process through audits, self-assessments, penetration tests, and vulnerability assessments. 5. A validation though audits, self-assessments, penetration tests, and vulnerability assessments that risk decisions are informed by appropriate identification and analysis of threats and other potential causes of loss. The organization implements threat modeling (e.g., development of attack trees) as part of its risk assessment process to assist in identifying and quantifying risk in better understanding the nature frequency, and sophistication of threats.

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation:	The agency conducts, periodically, but at least annually, an assessment of the security controls in the systems that receive, store, process or transmit FTI, including cloud environments immediately prior to implementation of the cloud environment and during each annual risk assessment (or update to an existing risk assessment) thereafter.

	The agency ensures each aspect of a data warehouse is assessed for risk, including hardware, software, data transport, and data storage. Any risk documents identifies and documents all vulnerabilities, associated with a data warehousing environment.

Level GDPR Implementation Requirements	
Level GDPR Implementation:	Unless (i) processing has a legal basis in EU law or the law of the Member State to which the controller is subject; (ii) that law regulates the processing in question; and (iii) a data impact assessment has already been carried out as part of a general impact assessment, then where data processing is likely to result in a high risk to the rights and liberties (freedoms) of natural persons, the controller prior to processing carries out an assessment of the impact of said processing on the protection of personal data, taking into account the nature, scope, context and purposes of the processing. A single assessment may address a set of similar processing operations that present similar high risks. Where necessary, the controller carries out a review to assess if processing is performed in accordance with the data impact assessment, at least when there is a change in the risk represented by processing operations. A data protection impact assessment is required in the case of: 1. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions; 2. are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; 3. processing on a large scale of special categories of personal data, or of personal data relating to criminal convictions and offences; or 4. a systematic monitoring of a publicly accessible area on a large scale. The controller seeks the advice of the data protection officer, where designated, when carrying out a data protection impact assessment and, where appropriate, seeks out the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations. Data protection impact assessments contain at least: 1. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; 2. an assessment of the necessity and proportionality of the processing operations in relation to the purposes; 3. an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and 4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the EU GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned. The controller consults the supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. When consulting the supervisory authority, the controller provides the supervisory authority with: 1. where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

	2. the purposes and means of the intended processing; 3. the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to the EU GDPR; 4. where applicable, the contact details of the data protection officer; 5. the data protection impact assessment; and 6. any other information requested by the supervisory authority.

Level HIPAA Implementation Requirements

Level HIPAA Implementation:	Risk assessments (analyses), which are used to determine if a breach of unsecured protected health information (PHI) is reportable to Secretary of Health and Human Services, must demonstrate there is a low probability of compromise (lo pro co) rather than a significant risk of harm. The terms breach and PHI are as defined by the Secretary. The methodology, at a minimum, addresses the following factors: 1. the nature of the PHI involved, including the types of identifiers involved and the likelihood 2. e-identification; 3. the unauthorized person who used the PHI or to whom the disclosure was made; 4. whether the PHI was actually acquired or viewed; 5. the extent to which the risk to the PHI has been mitigated; and 6. and other factors/guidance promulgated by the Secretary.

Level HIX Implementation Requirements

Level HIX Implementation:	The organization: 1. Develops a documented security and privacy assessment plan that describes the scope of the assessment, including security and privacy controls and control enhancements under the assessment, assessment procedures to be used to determine control effectiveness, and the assessment environment, assessment team, and assessment roles and responsibilities; 2. Assesses the security and privacy controls in the information system within every 365 days in accordance with the current Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the established security and privacy requirements; 3. Produces an assessment report that documents the result of the assessment; and 4. Provides the results of the security and privacy control assessment within every 365 days, in writing, to the Business Owner who is responsible for reviewing the assessment documentation and update system security documentation where necessary to reflect any changes to the system. A security and privacy assessment of all security and privacy controls must be conducted prior to issuing the authority to operate for all newly implemented, or significantly changed systems. The annual security assessment requirement mandated by CMS requires all Minimum-Security Controls attributable to a system or application to be assessed over a three-year period. To meet this requirement, a subset of the Minimum Acceptable Risk Controls for Exchanges is tested each year so that all security controls are tested during a three-year period.

	The Business Owner notifies the CMS within 30 days whenever updates are made to system security and privacy authorization artifacts or when significant role changes occur (e.g., Business Owner, System Developer/Maintainer, ISSO). An independent assessment of all security and privacy controls is conducted every three years or with each major system change.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The organization (i) conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; (ii) conducts an E-Authentication Risk Assessment (ERA), as required, on systems and determines e-authentication assurance levels; (iii) documents risk assessment results in the applicable security plan; (iv) reviews risk assessment results within every 365 days; (v) disseminates risk assessment results to affected stakeholders, Business Owners(s), and the CMS CISO; and (vi) updates the risk assessment before issuing a new authority to operate (ATO) package or within every three [3] years, whichever comes first, or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system. Systems processing, storing, or transmitting PII (to include PHI): Include an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of personally identifiable information (PII) in the related risk assessment documentation. Systems processing, storing, or transmitting PHI: The organization documents risk assessment results in a HIPAA Risk Analysis, and associated risks to PHI must be identified within the overall risk assessment, and all risk assessment documentation must reflect these findings; all HIPAA Risk Analysis documentation must be maintained for six [6] years from the date of creation or date it was last in effect – whichever is later. Information technology components that do not support host-based IDS/IPS sensors capability must be documented in the applicable risk assessment and security plan. Devices and appliances that do not support a host-based intrusion detection system/intrusion prevention system (IDS/IPS) sensor capability must be documented in the applicable risk assessment and security plan.

Level PCI Implementation Requirements

Level PCI Implementation:	Formal risk assessments are performed at least annually and upon significant changes to the environment. The assessments identify critical assets, threats and vulnerabilities and result in a formal, documented analysis of risk.

Control Reference: 03.c Risk Mitigation

Control Specification:	Risks shall be mitigated to an acceptable level. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Documentation and Records; IT Organization and Management Roles and Responsibilities; Risk Management and Assessments

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 2 Subject to CMMC Level 3 Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Basic Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Texas Health and Safety Code Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	Risks can be dealt with in one of four ways: 1. Avoidance - This approach eliminates the risk by avoidance of the activity which provides the risk. For example, the risk associated with utilization of wireless technologies can be mitigated by deciding not to use wireless technologies at all. 2. Reduction - Risk can be reduced by way of controls that can reduce the likelihood or impact of a risk. An example would be encryption of network traffic to minimize risks that threaten the confidentiality of data. 3. Transference - Risk can be reduced by shifting it to an outside entity. An example would be the purchase of insurance against fire damage. 4. Acceptance - Organizations can choose to accept risk by not selecting any of the aforementioned approaches. When acceptance is selected, management acceptance must be documented. Organizations define and document the criteria to determine whether or not a risk is avoided, accepted, transferred or treated. The factors to be taken into account include the following: 1. industry sector, industry or organizational laws, regulations, and standards; 2. contractual, business, or other priorities; 3. cultural fit; 4. customer/client concerns; 5. coherence with IT, corporate risk acceptance, and business strategy; 6. cost; 7. effectiveness; 8. type of protection; 9. number of threats covered; 10. risk level at which the controls become justified; 11. risk level that led to the recommendation being made; 12. alternatives already in place; and 13. additional benefits derived. The organization implements a process for ensuring that corrective action plans for the security program and the associated organizational information systems are prioritized and maintained; and the remedial information security actions necessary to mitigate risk

	to organizational operations and assets, individuals, and other organizations are documented. The organization reviews corrective action plans (plans of action and milestones) for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. The organization updates existing remediation or corrective action plans monthly based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. The organization mitigates any harmful effect that is known to the organization of a use or disclosure of covered information (e.g., PII) by the organization or its business partners, vendors, contractors, or similar third-party, in violation of its policies and procedures. The organization implements an integrated control system characterized using different control types (e.g., layered, preventative, detective, corrective, and compensating) that mitigates identified risks.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.530(f) HIPAA.PR AICPA 2017 CC4.2 AICPA 2017 CC5.1 AICPA 2017 P6.4 AICPA 2017 P6.5 AICPA 2017 P6.6 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMMC v1.0 CA.2.159-0 CMMC v1.0 RM.3.144-2 CMSRs v3.1 CA-05 (HIGH; MOD) CMSRs v3.1 PM-04 (HIGH; MOD) CRR v2016 CCM:MIL3.Q4 CRR v2016 CM:G1.Q2 CRR v2016 CM:G4.Q2 CRR v2016 EDM:MIL3.Q4 CRR v2016 IM:MIL3.Q4 CRR v2016 RM:G1.Q3 CRR v2016 RM:G2.Q3 CRR v2016 RM:G4.Q2 CRR v2016 RM:MIL2.Q4 CRR v2016 SA:MIL3.Q4 CRR v2016 TA:MIL3.Q4 CRR v2016 VM:MIL3.Q4 CSA CCM v3.0.1 GRM-11 FedRAMP CA-5 FFIEC IS v2016 A.6.4 FFIEC IS v2016 A.6.4(a) FFIEC IS v2016 A.7.1 FFIEC IS v2016 A.7.2 FFIEC IS v2016 A.7.3 IRS Pub 1075 v2016 9.3.4.4 MARS-E v2 CA-5 MARS-E v2 CA-5(1) MARS-E v2 PM-4 NIST 800-171 r2 3.12.2-0 NIST Cybersecurity Framework v1.1 ID.RA-6 NIST Cybersecurity Framework v1.1 PR.IP-12 NIST Cybersecurity Framework v1.1 RS.MI-3 NIST SP 800-53 R4 CA-2(3)[S]{0} NIST SP 800-53 R4 CA-5a[HML]{0} NIST SP 800-53 R4 PL-8(1)a[S]{0} NIST SP 800-53 R4 PM-4a[HML]{1} NIST SP 800-53 R4 SC-3(5)[S]{0} NY DOH SSP v3.1 PM-11.PII[M]-1 NY DOH SSP v3.1 PM-4a2[M]-0

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CMMC Level 3 Subject to CRR V2016 Subject to FedRAMP Certification Subject to HIPAA Security Rule Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate)
Level 2 Implementation:	Level 1 plus: The organization develops a formal mitigation plan that includes: 1. performing a cost/benefit analysis for identified countermeasures; 2. documenting a risk treatment plan which provides recommended countermeasures to management; 3. documenting and presenting risk treatment summary reports to management; 4. management approving countermeasures documented in the risk treatment plan; 5. mapping decisions taken against the list of HITRUST CSF controls; 6. plans for implementations (current and future) documented in the organization's security improvement plan; and 7. implementing the management-approved risk treatment plan; 8. continually assessing the capability of technology needed to sustain an appropriate level of information security based on the size, complexity, and risk appetite of the organization.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.308(a)(1)(ii)(B) HIPAA.SR-0 AICPA 2017 CC4.2 CMMC v1.0 RM.3.146-0 CMSRs v3.1 CA-05 (HIGH; MOD) CRR v2016 CM:G4.Q1 CRR v2016 RM:MIL3.Q1 CRR v2016 RM:MIL4.Q1 CRR v2016 RM:MIL4.Q2 CRR v2016 RM:MIL5.Q2 CRR v2016 VM:G3.Q1 CRR v2016 VM:G3.Q2 CRR v2016 VM:G4.Q1 CSA CCM v3.0.1 GRM-11 FedRAMP CA-5 FFIEC IS v2016 A.6.4 FFIEC IS v2016 A.7.1 FFIEC IS v2016 A.7.2 FFIEC IS v2016 A.7.3 IRS Pub 1075 v2016 9.3.4.4 ISO/IEC 27002:2013 12.6.1 ISO/IEC 27002:2013 12.7.1

	ISO/IEC 27002:2013 17.1.1 ISO/IEC 27799:2016 12.6.1 ISO/IEC 27799:2016 12.7.1 ISO/IEC 27799:2016 17.1.1 MARS-E v2 CA-5 NIST Cybersecurity Framework v1.1 ID.RA-6 NIST Cybersecurity Framework v1.1 PR.IP-12 NIST SP 800-53 R4 CA-5b[HML]{0} NIST SP 800-53 R4 PM-4b[HML]{0}

Level CMS Implementation Requirements

Level CMS Implementation:	The organization employs automated mechanisms to help ensure that the POA&M for the information system is accurate, up to date, and readily available. The organization: 1. develops and submits a Plan of Action and Milestones (POA&M) for the information system within 30 days of the final results for every internal/external audit/review or test (e.g., ST&E, penetration test) to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls, and to reduce or eliminate known vulnerabilities in the system; and 2. updates and submits existing POA&M monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The organization updates the Plan of Action and Milestones (POA&M) at least monthly based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Level FFIEC IS Implementation Requirements

Level FFIEC IS Implementation:	The organization implements processes to measure risks to guide its recommendations for and use of mitigating controls using threat analysis tools (e.g., event trees, attack trees, kill chains) in understanding and supporting the measurement of information security risks. Such tools: 1. Map threats and vulnerabilities 2. Incorporate legal and regulatory requirements 3. Improve consistency in risk measurement 4. Identify areas for mitigation 5. Allow comparisons among different threats, events, and potential mitigating controls

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	The agency must submit an updated Corrective Action Plan (CAP) twice each year to address corrective actions identified during an on-site safeguards review until all findings are closed. The CAP is submitted as an attachment to the SAR, and on the CAP due date which is six months from the scheduled SAR due date.

Level HIX Implementation Requirements

Level HIX Implementation:	The organization employs automated mechanisms to help ensure that the POA&M for the information system is accurate, up to date, and readily available.

Control Reference: 03.d Risk Evaluation

Control Specification:	Risks shall be continually evaluated and assessed. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	IT Organization and Management Roles and Responsibilities; Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation:	The risk management program includes the requirement that risk assessments be re-evaluated at least annually, or when there are significant changes in the environment.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC3.4 AICPA 2017 CC4.1 CMSRs v3.1 RA-03 (HIGH; MOD) CRR v2016 RM:MIL4.Q2 CRR v2016 RM:MIL4.Q3 FedRAMP RA-3 FFIEC IS v2016 A.7.1 IRS Pub 1075 v2016 9.3.14.2 MARS-E v2 RA-3 NIST Cybersecurity Framework v1.1 ID.RA-1 NIST Cybersecurity Framework v1.1 ID.RA-3 NIST Cybersecurity Framework v1.1 ID.RA-4 NIST Cybersecurity Framework v1.1 ID.RA-5

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CMMC Level 2

	Subject to FedRAMP Certification Subject to FISMA Compliance Subject to FTC Red Flags Rule Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The risk management process is integrated with the change management process within the organization, and risk assessments conducted whenever there is a significant change in the environment, or there is a change that could have a significant impact. Results of the risk assessments are included in the change management process, so they may guide the decisions within the change management process (e.g., approvals for changes). The organization updates the risk assessment: 1. before issuing a new formal authorization to operate or within every three years, whichever comes first; or 2. whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities); or 3. other conditions that may impact the security or authorization state of the system. The privacy, security and risk management program(s) are updated to reflect changes in risks based on: 1. any experiences with security incidents, weaknesses, breaches, or identity theft; 2. changes in the environment (e.g., new methods of attack, new sources of attack, new vulnerabilities); 3. changes in prevention, detection, or response methods for security; 4. changes within the organization including: i. organizational mergers, acquisitions, alliances, joint ventures, or service provider arrangements; ii. new systems or facilities; iii. new service offerings; and iv. new types of accounts.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(3) 1 TAC § 390.2(a)(4)(A)(xi) 16 CFR Part § 681 Appendix A V 16 CFR Part § 681 Appendix A V(a) 16 CFR Part § 681 Appendix A V(b) 16 CFR Part § 681 Appendix A V(c) 16 CFR Part § 681 Appendix A V(d) 16 CFR Part § 681 Appendix A V(e) AICPA 2017 CC3.4 AICPA 2017 CC8.1 CMMC v1.0 CM.2.066-0 CMSRs v3.1 CM-03 (HIGH; MOD) CMSRs v3.1 RA-03 (HIGH; MOD) CSA CCM v3.0.1 GRM-08 FedRAMP CM-3 FedRAMP RA-3 FFIEC IS v2016 A.7.1 IRS Pub 1075 v2016 9.3.14.2 ISO/IEC 27002:2013 12.1.2 ISO/IEC 27799:2016 12.1.2 MARS-E v2 CM-3 MARS-E v2 RA-3 NIST 800-171 r2 3.4.4-0

	NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 ID.RA-1 NIST Cybersecurity Framework v1.1 ID.RA-3 NIST Cybersecurity Framework v1.1 ID.RA-4 NIST Cybersecurity Framework v1.1 ID.RA-5 NY DOH SSP v3.1 PM-14.PII[M]-3 NY DOH SSP v3.1 PM-9c[M]-1

Control Category: 04.0 - Security Policy

Objective Name: 04.01 Information Security Policy

Control Objective:	To provide management direction in line with business objectives and relevant laws and regulations, demonstrate support for, and commitment to information security through the issue and maintenance of information security policies across the organization.

Control Reference: 04.a Information Security Policy Document

Control Specification:	Information Security Policy documents shall be approved by management and published and communicated to all employees and relevant external parties. Information Security Policy documents shall establish the direction of the organization and align to best practices, regulatory, federal/state, and international laws where applicable. The Information Security policy documents shall be supported by a strategic plan and a security program with well-defined roles and responsibilities for leadership and officer roles. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Awareness and Training; Contingency Planning; Documentation and Records; IT Organization and Management Roles and Responsibilities; Policies and Procedures; Requirements (Legal and Contractual); Third-parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to HIPAA Security Rule Subject to IRS Pub 1075 Compliance Subject to Joint Commission Accreditation Subject to MARS-E Requirements Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to Texas Health and Safety Code Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	Information security policy documents are developed, published, disseminated, and implemented. The information security policy documents state the purpose and scope of the policy, communicate management's commitment, describe management and workforce member's roles and responsibilities, and establish the organization's approach to managing information security. As applicable to the focus of a particular document, policies contain: 1. The organizations mission, vision, values, objectives, activities, and purpose, including the organizations place in critical infrastructure; 2. a definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing;

3. a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;
4. a framework for setting control objectives and controls, including the structure of risk assessment and risk management;
5. the need for information security;
6. the goals of information security;
7. compliance scope;
8. legislative, regulatory, and contractual requirements, including those for the protection of covered information, and the legal and ethical responsibilities to protect this information;
9. arrangements for notification of information security incidents, including a channel for raising concerns regarding confidentially, without fear of blame or recrimination.
10. a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including but not limited to CSF control objectives such as:
    i. compliance with legislative, regulatory, and contractual requirements;
    ii. security education, training, and awareness requirements for the workforce, including researchers and research participants;
    iii. incident response and business continuity management;
    iv. consequences of information security policy violations;
    v. continuous monitoring;
    vi. designating and maintaining an appropriately resourced and technically experienced information security team;
    vii. physical security of areas where sensitive information (e.g., ePHI, PCI, and PMI data); and
    viii. coordination among organizational entities;
11. a definition of general and specific responsibilities for information security management, including reporting information security incidents;
12. prescribes the development, dissemination, and review/update of formal, documented procedures to facilitate the implementation of security policy and associated security controls; and
13. references to documentation which may support the policy (e.g., more detailed security policies and procedures for specific information systems or security rules users to comply with).

These information security policy documents are communicated throughout the organization to users in a form that is relevant, accessible, and understandable to the intended reader.

In the instance of any acquisitions, re-organizations, or mergers, or where the organization obtains support from third-party organizations or collaborates with third-parties, and especially if these activities involve other jurisdictions, the policy framework includes documented policy, controls, and procedures that cover such interactions and that specifies the responsibilities of all parties.

Level 1 Control Standard Mapping:

1 TAC § 390.2(a)(1)
1 TAC § 390.2(a)(4)(A)(xi)
45 CFR Part § 164.308(a)(1)(i) HIPAA.SR-0
45 CFR Part § 164.316(b)(2)(ii) HIPAA.SR-0
45 CFR Part § 164.530(i) HIPAA.PR
AICPA 2017 CC1.3
AICPA 2017 CC2.2
AICPA 2017 CC2.3
AICPA 2017 CC3.1
AICPA 2017 CC5.1
CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4
CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4
CMSRs v3.1 AC-01 (HIGH; MOD)
CMSRs v3.1 AT-01 (HIGH; MOD)
CMSRs v3.1 AU-01 (HIGH; MOD)
CMSRs v3.1 CA-01 (HIGH; MOD)
CMSRs v3.1 CM-01 (HIGH; MOD)

CMSRs v3.1 CP-01 (HIGH; MOD)
CMSRs v3.1 IA-01 (HIGH; MOD)
CMSRs v3.1 MA-01 (HIGH; MOD)
CMSRs v3.1 PE-01 (HIGH; MOD)
CMSRs v3.1 PL-01 (HIGH; MOD)
CMSRs v3.1 PM-01 (HIGH; MOD)
CMSRs v3.1 PS-01 (HIGH; MOD)
CMSRs v3.1 RA-01 (HIGH; MOD)
CMSRs v3.1 SA-01 (HIGH; MOD)
CMSRs v3.1 SC-01 (HIGH; MOD)
CMSRs v3.1 SI-01 (HIGH; MOD)
COBIT 5 APO13.02
COBIT 5 DS5.2
CRR v2016 AM:G1.Q3
CRR v2016 AM:MIL5.Q1
CRR v2016 CCM:MIL5.Q1
CRR v2016 CM:G1.Q1
CRR v2016 CM:G2.Q1
CRR v2016 CM:MIL2.Q1
CRR v2016 CM:MIL5.Q1
CRR v2016 EDM:MIL5.Q1
CRR v2016 IM:MIL5.Q1
CRR v2016 RM:MIL2.Q2
CRR v2016 RM:MIL5.Q1
CRR v2016 SA:MIL2.Q2
CRR v2016 SA:MIL2.Q4
CRR v2016 SA:MIL5.Q1
CRR v2016 SCM:MIL5.Q1
CRR v2016 TA:MIL5.Q1
CRR v2016 VM:MIL5.Q1
CSA CCM v3.0.1 GRM-06
FedRAMP AT-1
FedRAMP AU-1
FedRAMP CA-1
FedRAMP CM-1
FedRAMP CP-1
FedRAMP IA-1
FedRAMP IR-1
FedRAMP MA-1
FedRAMP MP-1
FedRAMP PE-1
FedRAMP PL-1
FedRAMP PS-1
FedRAMP RA-1
FedRAMP SA-1
FedRAMP SC-1
FedRAMP SI-1
HITRUST
IRS Pub 1075 v2016 9.3.1.1
IRS Pub 1075 v2016 9.3.10.1
IRS Pub 1075 v2016 9.3.11.1
IRS Pub 1075 v2016 9.3.12.1
IRS Pub 1075 v2016 9.3.13.1
IRS Pub 1075 v2016 9.3.14.1
IRS Pub 1075 v2016 9.3.15.1
IRS Pub 1075 v2016 9.3.16.1
IRS Pub 1075 v2016 9.3.17.1
IRS Pub 1075 v2016 9.3.2.1
IRS Pub 1075 v2016 9.3.3.1
IRS Pub 1075 v2016 9.3.4.1
IRS Pub 1075 v2016 9.3.5.1
IRS Pub 1075 v2016 9.3.6.1
IRS Pub 1075 v2016 9.3.7.1
IRS Pub 1075 v2016 9.3.8.1
IRS Pub 1075 v2016 9.3.9.1
IRS Pub 1075 v2016 Exhibit 10
ISO/IEC 27002:2013 5.1.1
ISO/IEC 27799:2016 5.1.1
MARS-E v2 AC-1
MARS-E v2 AT-1
MARS-E v2 AU-1
MARS-E v2 CA-1
MARS-E v2 CM-1
MARS-E v2 CP-1
MARS-E v2 IA-1

	MARS-E v2 IR-1 MARS-E v2 MA-1 MARS-E v2 PE-1 MARS-E v2 PL-1 MARS-E v2 PM-1 MARS-E v2 PS-1 MARS-E v2 RA-1 MARS-E v2 SC-1 MARS-E v2 SI-1 NIST Cybersecurity Framework v1.1 ID.GV-1 NIST Cybersecurity Framework v1.1 ID.GV-2 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 ID.GV-4 NY DOH SSP v3.1 PL-8a1[M]-0 PMI DSP Framework ID-1 TJC IM.02.01.03, EP 1

Level DGF Implementation Requirements

Level DGF Implementation:	Data Governance policies, rules, and standards are explicitly defined, documented, and communicated.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	The organization develops and disseminates a formal, documented, system and services acquisition policy that includes IRS documents received and identified by: 1. taxpayer name; 2. tax year(s); 3. type of information (e.g., revenue agent reports, Form 1040, work papers); 4. the reason for the request; 5. date requested; 6. date received; 7. exact location of the FTI; 8. who has had access to the data, and; 9. if disposed of, the date and method of disposition. The organization describes the purpose or function of a data warehouse in organizational policy.

Level PCI Implementation Requirements

Level PCI Implementation:	The organization ensures policies are documented, communicated (known to all parties) and in use for the following: 1. managing firewalls, 2. managing vendor defaults and other security parameters, 3. protecting stored cardholder data, 4. encrypting transmissions of cardholder data, 5. protecting systems against malware, 6. developing and maintaining secure systems and applications, 7. restricting access to cardholder data, 8. identification and authentication, 9. restricting physical access to cardholder data, 10. monitoring access to network resources and cardholder data, and 11. security monitoring and testing.

Control Reference: 04.b Review of the Information Security Policy

Control Specification:	The information security policy documents shall be reviewed at planned intervals or if significant changes occur to ensure its continuing adequacy and effectiveness. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Audit and Accountability; Documentation and Records; IT Organization and Management Roles and Responsibilities; Policies and Procedures

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to HIPAA Security Rule Subject to Texas Health and Safety Code
Level 1 Implementation:	The information security policy documents are reviewed at planned intervals or if significant changes occur to ensure the policies' continuing adequacy and effectiveness. Additional factors when developing or changing a security policy document include, but are not limited to, regulatory mandates, accreditation requirements, and industry best practices, e.g., for system and services development and acquisition. A process is defined and implemented for individuals to make complaints concerning the information security policies and procedures or the organization's compliance with the policies and procedures. All complaints and requests for changes are documented, including their disposition, if any. These information security policy documents are communicated throughout the organization to users in a form that is relevant, accessible, and understandable to the intended reader.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.316(b)(2)(iii) HIPAA.SR-2 45 CFR Part § 164.530(d)(1) HIPAA.PR 45 CFR Part § 164.530(i) HIPAA.PR AICPA 2017 CC1.4 AICPA 2017 CC5.2 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 AC-01 (HIGH; MOD) CMSRs v3.1 AR-02 (HIGH; MOD) CMSRs v3.1 AT-01 (HIGH; MOD) CMSRs v3.1 AU-01 (HIGH; MOD) CMSRs v3.1 CA-01 (HIGH; MOD) CMSRs v3.1 CM-01 (HIGH; MOD) CMSRs v3.1 CP-01 (HIGH; MOD) CMSRs v3.1 IA-01 (HIGH; MOD) CMSRs v3.1 IP-04 (HIGH; MOD) CMSRs v3.1 MA-01 (HIGH; MOD) CMSRs v3.1 PE-01 (HIGH; MOD) CMSRs v3.1 PL-01 (HIGH; MOD) CMSRs v3.1 PM-01 (HIGH; MOD) CMSRs v3.1 PS-01 (HIGH; MOD) CMSRs v3.1 RA-01 (HIGH; MOD) CMSRs v3.1 SA-01 (HIGH; MOD) CMSRs v3.1 SC-01 (HIGH; MOD) CMSRs v3.1 SI-01 (HIGH; MOD) CRR v2016 CM:G4.Q1 CSA CCM v3.0.1 GRM-09

	FedRAMP AT-1 FedRAMP AU-1 FedRAMP CA-1 FedRAMP CM-1 FedRAMP CP-1 FedRAMP IA-1 FedRAMP IR-1 FedRAMP MA-1 FedRAMP MP-1 FedRAMP PE-1 FedRAMP PL-1 FedRAMP PS-1 FedRAMP RA-1 FedRAMP SA-1 FedRAMP SC-1 FedRAMP SI-1 IRS Pub 1075 v2016 9.3.1.1 IRS Pub 1075 v2016 9.3.10.1 IRS Pub 1075 v2016 9.3.11.1 IRS Pub 1075 v2016 9.3.12.1 IRS Pub 1075 v2016 9.3.13.1 IRS Pub 1075 v2016 9.3.14.1 IRS Pub 1075 v2016 9.3.15.1 IRS Pub 1075 v2016 9.3.16.1 IRS Pub 1075 v2016 9.3.2.1 IRS Pub 1075 v2016 9.3.3.1 IRS Pub 1075 v2016 9.3.4.1 IRS Pub 1075 v2016 9.3.5.1 IRS Pub 1075 v2016 9.3.6.1 IRS Pub 1075 v2016 9.3.7.1 IRS Pub 1075 v2016 9.3.8.1 IRS Pub 1075 v2016 9.3.9.1 IRS Pub 1075 v2016 Exhibit 10 ISO/IEC 27002:2013 5.1.2 ISO/IEC 27799:2016 5.1.2 MARS-E v2 AC-1 MARS-E v2 AR-1 MARS-E v2 AR-2 MARS-E v2 AT-1 MARS-E v2 AU-1 MARS-E v2 CA-1 MARS-E v2 CM-1 MARS-E v2 CP-1 MARS-E v2 IA-1 MARS-E v2 IR-1 MARS-E v2 MA-1 MARS-E v2 PE-1 MARS-E v2 PL-1 MARS-E v2 PM-1 MARS-E v2 PS-1 MARS-E v2 RA-1 MARS-E v2 SC-1 MARS-E v2 SI-1 NIST Cybersecurity Framework v1.1 ID.GV-1 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 ID.GV-4 PMI DSP Framework ID-1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records

Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to CRR V2016 Subject to FedRAMP Certification Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The information security policy documents are reviewed at planned intervals, at a minimum every 365 days, or if significant changes occur in the operating or business environment to ensure its continuing adequacy and effectiveness and that the totality of the policy has been addressed at least every 365 days. The information security policy documents have an owner who has approved management responsibility for the development, review, and evaluation of the security policy. The review includes assessing opportunities for improvement of the organization's information security policy documents and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions, or technical environment. The input to the management review includes information on: 1. feedback from interested parties; 2. results of independent reviews (see 5.h); 3. status of preventive and corrective actions (see 5.h and 6.g); 4. results of previous management reviews; 5. process performance and information security policy compliance; 6. changes that could affect the organization's approach to managing information security, including changes to the organizational environment, business circumstances, resource availability, contractual, regulatory, and legal conditions, or to the technical environment; 7. trends related to threats and vulnerabilities; 8. reported information security incidents (see 11.a); and 9. recommendations provided by relevant authorities (see 5.f). The output from the management review includes any decisions and actions related to: 1. improvement of the organization's approach to managing information security and its processes; 2. improvement of control objectives and controls; and 3. improvement in the allocation of resources and/or responsibilities. A record of the management review is maintained. Management approval for the revised policy documents is obtained.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.530(i)(2) HIPAA.PR 45 CFR Part § 164.530(i)(3) HIPAA.PR 45 CFR Part § 164.530(i)(5) HIPAA.PR AICPA 2017 CC5.3 CMSRs v3.1 AC-01 (HIGH; MOD) CMSRs v3.1 AT-01 (HIGH; MOD) CMSRs v3.1 AU-01 (HIGH; MOD) CMSRs v3.1 CA-01 (HIGH; MOD) CMSRs v3.1 CM-01 (HIGH; MOD) CMSRs v3.1 CP-01 (HIGH; MOD) CMSRs v3.1 IA-01 (HIGH; MOD) CMSRs v3.1 MA-01 (HIGH; MOD)

	CMSRs v3.1 PE-01 (HIGH; MOD) CMSRs v3.1 PL-01 (HIGH; MOD) CMSRs v3.1 PM-01 (HIGH; MOD) CMSRs v3.1 PS-01 (HIGH; MOD) CMSRs v3.1 RA-01 (HIGH; MOD) CMSRs v3.1 SA-01 (HIGH; MOD) CMSRs v3.1 SC-01 (HIGH; MOD) CMSRs v3.1 SI-01 (HIGH; MOD) FedRAMP AT-1 FedRAMP AU-1 FedRAMP CA-1 FedRAMP CM-1 FedRAMP CP-1 FedRAMP IA-1 FedRAMP IR-1 FedRAMP MA-1 FedRAMP MP-1 FedRAMP PE-1 FedRAMP PL-1 FedRAMP PS-1 FedRAMP RA-1 FedRAMP SA-1 FedRAMP SC-1 FedRAMP SI-1 IRS Pub 1075 v2016 9.3.1.1 IRS Pub 1075 v2016 9.3.10.1 IRS Pub 1075 v2016 9.3.11.1 IRS Pub 1075 v2016 9.3.12.1 IRS Pub 1075 v2016 9.3.13.1 IRS Pub 1075 v2016 9.3.14.1 IRS Pub 1075 v2016 9.3.15.1 IRS Pub 1075 v2016 9.3.16.1 IRS Pub 1075 v2016 9.3.17.1 IRS Pub 1075 v2016 9.3.2.1 IRS Pub 1075 v2016 9.3.3.1 IRS Pub 1075 v2016 9.3.4.1 IRS Pub 1075 v2016 9.3.5.1 IRS Pub 1075 v2016 9.3.6.1 IRS Pub 1075 v2016 9.3.7.1 IRS Pub 1075 v2016 9.3.8.1 IRS Pub 1075 v2016 9.3.9.1 ISO/IEC 27002:2013 5.1.2 ISO/IEC 27799:2016 5.1.2 MARS-E v2 AC-1 MARS-E v2 AT-1 MARS-E v2 AU-1 MARS-E v2 CA-1 MARS-E v2 CM-1 MARS-E v2 CP-1 MARS-E v2 IA-1 MARS-E v2 IR-1 MARS-E v2 MA-1 MARS-E v2 PE-1 MARS-E v2 PL-1 MARS-E v2 PM-1 MARS-E v2 PS-1 MARS-E v2 RA-1 MARS-E v2 SC-1 MARS-E v2 SI-1 NIST Cybersecurity Framework v1.1 ID.GV-1 NIST Cybersecurity Framework v1.1 ID.GV-3 NRS 603A.215.1 NY DOH SSP v3.1 PM-2.IS.PHI1[M]-1 PCI DSS v3.2.1 12.1.1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB)

	Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to Banking Requirements Subject to EHNAC Accreditation
Level 3 Implementation:	Level 2 plus: The review addresses the following: 1. the changing nature of the organization's operations and thus risk profile and risk management needs; 2. the changes made to the IT infrastructure of the organization, with the changes these bring to the organization's risk profile; 3. the changes identified in the external environment that similarly impact the organizations risk profile; 4. the latest controls, compliance and assurance requirements and arrangements of national bodies and of new legislation or regulation; 5. the latest guidance and recommendations from professional associations and from information privacy commissioners regarding the protection of covered information; 6. the results of legal cases tested in courts, that thereby establish or cancel precedents and established practices; and 7. the challenges and issues regarding the policy, as expressed to the organization by its staff, customers, and their partners and care givers, researchers, and governments, e.g., privacy commissioners.
Level 3 Control Standard Mapping:	45 CFR Part § 164.530(i)(2) HIPAA.PR 45 CFR Part § 164.530(i)(3) HIPAA.PR 45 CFR Part § 164.530(i)(5) HIPAA.PR FFIEC IS v2016 A.4.5 ISO/IEC 27002:2013 5.1.2 ISO/IEC 27799:2016 5.1.2 NIST Cybersecurity Framework v1.1 ID.GV-1 NIST Cybersecurity Framework v1.1 ID.GV-3

Level DGF Implementation Requirements

Level DGF Implementation:	Data Governance policies, rules, and standards are updated as needed or at least annually.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	The organization periodically reviews/updates a formal, documented, system and services acquisition policy that includes IRS documents received and identified by: 1. taxpayer name; 2. tax year(s); 3. type of information (e.g., revenue agent reports, Form 1040, work papers); 4. the reason for the request; 5. date requested; 6. date received; 7. exact location of the FTI; 8. who has had access to the data, and; 9. if disposed of, the date and method of disposition.

Control Category: 05.0 - Organization of Information Security

Objective Name: 05.01 Internal Organization

Control Objective:	To maintain the security of the organization's information and information assets (data centers or offices that process covered information).

Control Reference: 05.a Management Commitment to Information Security

Control Specification:	Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Audit and Accountability; Awareness and Training; IT Organization and Management Roles and Responsibilities; Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 4 Subject to FISMA Compliance Subject to HIPAA Security Rule Subject to IRS Pub 1075 Compliance Subject to Joint Commission Accreditation Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to State of Massachusetts Data Protection Act Subject to Texas Health and Safety Code Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	The organization's senior management: 1. appoints a senior-level information security official for the development, implementation, and administration of security matters; 2. establishes and communicates the organizations priorities for organizational mission, objectives, and activities; 3. ensures that the organization's information security processes are in place, are communicated to all stakeholders, and consider and address organizational requirements; 4. formally assigns an organization single point of contact or group to provide program oversight (governance), reviews and updates the organizations security plan (strategy, policies, etc.), ensures compliance with the security plan by the

	workforce, and evaluates and accepts information security risk on behalf of the organization (e.g., CEO, COO, Security Steering Committee, etc.); 5. formulates, reviews, and approves information security policies and a policy exception process; 6. periodically, at a minimum annually, reviews and assesses the effectiveness of the implementation of the information security policy; 7. provides clear direction and visible management support for security initiatives; 8. provides the resources needed for information security; 9. initiates plans and programs to maintain information security awareness; 10. ensures that all appropriate measures are taken to avoid cases of identity theft targeted at clients/customers, employees, and third-parties; 11. ensures that the implementation of information security controls is coordinated across the organization; and 12. determines and coordinates, as needed, internal or external information security specialists, and reviews and coordinates results of the specialists' advice throughout the organization. The organization: 1. ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement; 2. employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and 3. ensures that information security resources are available for expenditure as planned. If the senior-level information security official is employed by the organization, one of its affiliates, or a third-party service, the organization must: 1. retain responsibility for its cybersecurity program in compliance with applicable regulatory requirements; 2. designate a senior member of the organization’s personnel responsible for direction and oversight of the third-party service provider; and 3. require the third-party service to maintain a cybersecurity program that protects the organization and complies with applicable regulatory requirements.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 201 CMR 17.03(2)(a) 23 NYCRR 500.04(a)(1) 23 NYCRR 500.04(a)(2) 23 NYCRR 500.04(a)(3) 45 CFR Part § 164.308(a)(2) HIPAA.SR-0 AICPA 2017 CC2.2 AICPA 2017 CC3.1 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMMC v1.0 CA.4.163-0 CMSRs v3.1 PM-02 (HIGH; MOD) CMSRs v3.1 PM-03 (HIGH; MOD) COBIT 5 APO13.01 COBIT 5 APO13.02 COBIT 5 DS5.1 CRR v2016 AM:G1.Q4 CRR v2016 AM:MIL2.Q3 CRR v2016 AM:MIL3.Q1 CRR v2016 AM:MIL3.Q3 CRR v2016 AM:MIL4.Q3 CRR v2016 CCM:MIL2.Q3 CRR v2016 CCM:MIL3.Q1 CRR v2016 CCM:MIL3.Q3 CRR v2016 CCM:MIL4.Q3 CRR v2016 CM:MIL2.Q3 CRR v2016 CM:MIL3.Q1 CRR v2016 CM:MIL3.Q3 CRR v2016 CM:MIL4.Q3

	CRR v2016 EDM:MIL2.Q3 CRR v2016 EDM:MIL3.Q1 CRR v2016 EDM:MIL3.Q3 CRR v2016 EDM:MIL4.Q3 CRR v2016 IM:MIL4.Q3 CRR v2016 RM:MIL2.Q3 CRR v2016 RM:MIL3.Q1 CRR v2016 RM:MIL3.Q3 CRR v2016 RM:MIL4.Q3 CRR v2016 SA:G1.Q3 CRR v2016 SA:MIL2.Q3 CRR v2016 SA:MIL3.Q1 CRR v2016 SA:MIL3.Q3 CRR v2016 SA:MIL4.Q3 CRR v2016 SCM:MIL3.Q1 CRR v2016 SCM:MIL3.Q3 CRR v2016 SCM:MIL4.Q3 CRR v2016 TA:G2.Q6 CRR v2016 TA:MIL2.Q3 CRR v2016 TA:MIL3.Q1 CRR v2016 TA:MIL4.Q3 CRR v2016 VM:MIL2.Q3 CRR v2016 VM:MIL3.Q1 CRR v2016 VM:MIL3.Q3 CRR v2016 VM:MIL4.Q3 CSA CCM v3.0.1 GRM-05 De-ID Framework v1 Accountable Individuals: General De-ID Framework v1 Security Points of Contact: General FFIEC IS v2016 A.1.5 FFIEC IS v2016 A.2.10 FFIEC IS v2016 A.2.2 FFIEC IS v2016 A.2.3 FFIEC IS v2016 A.2.9 FFIEC IS v2016 A.6.4(b) IRS Pub 1075 v2016 9.3.18.1 ISO/IEC 27002:2013 5.1.1 ISO/IEC 27799:2016 5.1.1 MARS-E v2 PM-2 MARS-E v2 PM-3 NIST Cybersecurity Framework v1.1 ID.BE-3 NIST Cybersecurity Framework v1.1 ID.GV-1 NIST Cybersecurity Framework v1.1 ID.GV-2 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 ID.RM-1 NIST Cybersecurity Framework v1.1 PR.AT-4 NIST SP 800-53 R4 AC-3(4)[S]{2} NIST SP 800-53 R4 CM-3g[HM]{3} NIST SP 800-53 R4 PL-9[S]{0} NIST SP 800-53 R4 PM-3[HML]{0} NRS 603A.215.1 NY DOH SSP v3.1 PM-2[M]-0 NY DOH SSP v3.1 PM-3a[M]-0 NY DOH SSP v3.1 PM-3b[M]-0 NY DOH SSP v3.1 PM-3c[M]-0 PCI DSS v3.2.1 12.5 PCI DSS v3.2.1 12.5.1 PMI DSP Framework DE-5 PMI DSP Framework ID-1 TJC IM.02.01.03, EP 5

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters

	Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to 23 NYCRR 500 Subject to Banking Requirements Subject to CRR V2016 Subject to FTC Red Flags Rule Subject to NY OHIP Moderate-Plus Security Baseline
Level 2 Implementation:	Level 1 plus: The organization's senior management: 1. ensures that organization's information security strategy and goals are identified and considered, and addresses organizational and business-specific requirements, and verifies that appropriate processes are in place to meet the organization's strategy and goals; 2. formally reviews and approves in writing the establishment and administration of any information privacy, security, and risk management programs; 3. formally approves in writing the assignment of specific roles and responsibilities for information security across the organization; 4. ensures the senior security official can demonstrate professional competency in security matters via a recognized security industry certification, appropriate vendor certifications or a minimum of five years of security-related experience; 5. documents its risk acceptance process; and 6. conducts an annual review (may be performed by a third-party) of the effectiveness of its security program. The organization formally appoints in writing non-professional or professional security contacts by name in each major organizational area or business unit. The CISO of the organization must report in writing on the organization’s cybersecurity program and material cybersecurity risks at least annually to the organizations board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, reporting must be made to the individual or committee responsible for the organization's cybersecurity program. The report must include, to the extent applicable but is not limited to, the following: 1. The confidentiality of nonpublic information and the integrity and security of the organization’s information systems; 2. The organizations cybersecurity policies and procedures; 3. Material cybersecurity risks to the organization; 4. Overall effectiveness of the organization’s cybersecurity program; and 5. Material cybersecurity events involving the organization during the time period addressed by the report.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(3) 1 TAC § 390.2(a)(4)(A)(xi) 16 CFR Part § 681.1 (e)(1) 16 CFR Part § 681.1 (e)(2) 23 NYCRR 500.04(b) 23 NYCRR 500.04(b)(1) 23 NYCRR 500.04(b)(2) 23 NYCRR 500.04(b)(3) 23 NYCRR 500.04(b)(4) 23 NYCRR 500.04(b)(5) AICPA 2017 CC3.1 AICPA 2017 CC3.2 CMSRs v3.1 AR-01 (HIGH; MOD) CMSRs v3.1 PM-01 (HIGH; MOD) CMSRs v3.1 PM-02 (HIGH; MOD)

	CMSRs v3.1 PM-09 (HIGH; MOD) CMSRs v3.1 PM-13 (HIGH; MOD) CRR v2016 AM:MIL4.Q1 CRR v2016 AM:MIL4.Q2 CRR v2016 CCM:MIL3.Q2 CRR v2016 CCM:MIL4.Q1 CRR v2016 CCM:MIL4.Q2 CRR v2016 CM:MIL4.Q1 CRR v2016 CM:MIL4.Q2 CRR v2016 EDM:MIL4.Q1 CRR v2016 EDM:MIL4.Q2 CRR v2016 IM:MIL4.Q2 CRR v2016 RM:MIL3.Q2 CRR v2016 SA:MIL4.Q1 CRR v2016 SA:MIL4.Q2 CRR v2016 SCM:MIL4.Q2 CRR v2016 TA:G2.Q6 CRR v2016 TA:MIL4.Q1 CRR v2016 VM:MIL3.Q2 CRR v2016 VM:MIL4.Q1 CRR v2016 VM:MIL4.Q2 CSA CCM v3.0.1 GRM-04 CSA CCM v3.0.1 GRM-05 CSA CCM v3.0.1 GRM-11 FFIEC IS v2016 A.1.5 FFIEC IS v2016 A.2.2 FFIEC IS v2016 A.2.3 FFIEC IS v2016 A.2.6 FFIEC IS v2016 A.2.9 FFIEC IS v2016 A.6.2 HITRUST IRS Pub 1075 v2016 9.3.18.1 MARS-E v2 AR-1 MARS-E v2 PM-1 MARS-E v2 PM-13 MARS-E v2 PM-2 MARS-E v2 PM-9 NIST Cybersecurity Framework v1.1 ID.BE-2 NIST Cybersecurity Framework v1.1 ID.BE-3 NIST Cybersecurity Framework v1.1 ID.GV-1 NIST Cybersecurity Framework v1.1 ID.GV-2 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 PR.AT-4 NIST Cybersecurity Framework v1.1 PR.AT-5 NRS 603A.215.1 NY DOH SSP v3.1 PM-1b[M]-0 PCI DSS v3.2.1 12.5 PCI DSS v3.2.1 12.5.1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to FedRAMP Certification Subject to HITRUST De-ID Framework Requirements
Level 3 Implementation:	Level 2 plus:

	1. the organization formally creates a dedicated security management forum and publishes the forum's member list and charter. Such responsibilities can be handled by a Security Advisory Board, Security Steering Committee or by an existing management body, such as the board of directors; 2. the organization conducts an annual assessment of the effectiveness of its security program performed by a qualified outside organization; 3. the organization publishes security guidelines and/or daily operational procedures relating to processes that complement, clarify, and enforce security policies.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC1.4 AICPA 2017 CC2.2 AICPA 2017 CC5.3 CMSRs v3.1 AC-01 (HIGH; MOD) CMSRs v3.1 AT-01 (HIGH; MOD) CMSRs v3.1 AU-01 (HIGH; MOD) CMSRs v3.1 CA-01 (HIGH; MOD) CMSRs v3.1 CA-02 (HIGH; MOD) CMSRs v3.1 CA-02(01) (HIGH; MOD) CMSRs v3.1 CM-01 (HIGH; MOD) CMSRs v3.1 CP-01 (HIGH; MOD) CMSRs v3.1 IA-01 (HIGH; MOD) CMSRs v3.1 MA-01 (HIGH; MOD) CMSRs v3.1 PE-01 (HIGH; MOD) CMSRs v3.1 PL-01 (HIGH; MOD) CMSRs v3.1 PM-01 (HIGH; MOD) CMSRs v3.1 PS-01 (HIGH; MOD) CMSRs v3.1 RA-01 (HIGH; MOD) CMSRs v3.1 SA-01 (HIGH; MOD) CMSRs v3.1 SC-01 (HIGH; MOD) CMSRs v3.1 SI-01 (HIGH; MOD) CSA CCM v3.0.1 GRM-05 De-ID Framework v1 Governance: General FedRAMP AT-1 FedRAMP AU-1 FedRAMP CA-1 FedRAMP CA-2 FedRAMP CA-2(1) FedRAMP CM-1 FedRAMP CP-1 FedRAMP IA-1 FedRAMP IR-1 FedRAMP MA-1 FedRAMP PE-1 FedRAMP PL-1 FedRAMP PS-1 FedRAMP RA-1 FedRAMP SA-1 FedRAMP SC-1 FedRAMP SI-1 IRS Pub 1075 v2016 9.3.1.1 IRS Pub 1075 v2016 9.3.10.1 IRS Pub 1075 v2016 9.3.11.1 IRS Pub 1075 v2016 9.3.12.1 IRS Pub 1075 v2016 9.3.13.1 IRS Pub 1075 v2016 9.3.14.1 IRS Pub 1075 v2016 9.3.15.1 IRS Pub 1075 v2016 9.3.16.1 IRS Pub 1075 v2016 9.3.17.1 IRS Pub 1075 v2016 9.3.2.1 IRS Pub 1075 v2016 9.3.3.1 IRS Pub 1075 v2016 9.3.4.1 IRS Pub 1075 v2016 9.3.4.2 IRS Pub 1075 v2016 9.3.5.1 IRS Pub 1075 v2016 9.3.6.1 IRS Pub 1075 v2016 9.3.7.1 IRS Pub 1075 v2016 9.3.8.1 IRS Pub 1075 v2016 9.3.9.1 ISO/IEC 27002:2013 18.2.1 ISO/IEC 27002:2013 5.1.1 ISO/IEC 27799:2016 18.2.1 ISO/IEC 27799:2016 5.1.1

	MARS-E v2 AC-1 MARS-E v2 AT-1 MARS-E v2 AU-1 MARS-E v2 CA-1 MARS-E v2 CA-2 MARS-E v2 CA-2(1) MARS-E v2 CM-1 MARS-E v2 CP-1 MARS-E v2 IA-1 MARS-E v2 IR-1 MARS-E v2 MA-1 MARS-E v2 PE-1 MARS-E v2 PL-1 MARS-E v2 PM-1 MARS-E v2 PS-1 MARS-E v2 RA-1 MARS-E v2 SC-1 MARS-E v2 SI-1 NIST Cybersecurity Framework v1.1 ID.BE-2 NIST Cybersecurity Framework v1.1 ID.BE-3 NIST Cybersecurity Framework v1.1 ID.GV-2 NIST Cybersecurity Framework v1.1 ID.RM-1 PMI DSP Framework ID-3

Level DGF Implementation Requirements

Level DGF Implementation:	Compliance and success of the Data Governance program is evaluated at the organization and the application levels and reports on such attributes are shared with the leadership periodically. Individuals performing Data Governance work have the skills, experience, and necessary training to implement Data Governance processes/activities, as evidenced by knowledge of the tools, processes, corporate policies, and business expectations around management of the data.

Level PCI Implementation Requirements

Level PCI Implementation:	When being assessed as a service provider the organization's executive management establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: (i) overall accountability for maintaining PCI DSS compliance; and (ii) defining a charter for a PCI DSS compliance program and communication to executive management.

Control Reference: 05.b Information Security Coordination

Control Specification:	Information security activities shall be coordinated by representatives from different parts of the organization with relevant roles and job functions.
Factor Type:	Organizational
Topics:	Awareness and Training; IT Organization and Management Roles and Responsibilities; Personnel; Third-parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	

Level 1 Regulatory Factors:	Subject to Joint Commission Accreditation Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline
Level 1 Implementation:	The organization: 1. determines information security requirements for the information system in mission/business process planning; 2. determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; 3. establishes a discrete line item for information security in organizational programming and budgeting information; and 4. assigns authority and accountability to resources for communicating threat information. Information security coordination involves the active cooperation and collaboration across the entire organization. This activity: 1. ensures that security activities across the entire organization are executed in compliance with the information security policy and that deviations are identified and reviewed; 2. identifies how to handle non-compliance (such as sanctions or disciplinary action); 3. assesses the adequacy and coordinates the implementation of information security controls; 4. effectively promotes information security education, training, and awareness throughout the organization; and 5. ensures that threat information has been communicated to identified internal and external stakeholders. If the organization does not use a separate cross-functional group because such a group is not appropriate for the organization's size, the actions described above are undertaken by another suitable management body or individual security representative.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC1.1 AICPA 2017 CC3.1 CMSRs v3.1 PL-02(03) (HIGH; MOD) CMSRs v3.1 PM-01 (HIGH; MOD) CMSRs v3.1 PM-03 (HIGH; MOD) CMSRs v3.1 SA-02 (HIGH; MOD) COBIT 5 APO13.01 COBIT 5 APO13.02 COBIT 5 DS5.1 CRR v2016 AM:MIL2.Q3 CRR v2016 AM:MIL3.Q3 CRR v2016 AM:MIL4.Q3 CRR v2016 AM:MIL5.Q2 CRR v2016 CCM:MIL2.Q3 CRR v2016 CCM:MIL3.Q3 CRR v2016 CCM:MIL4.Q3 CRR v2016 CCM:MIL5.Q2 CRR v2016 CM:G2.Q1 CRR v2016 CM:MIL2.Q3 CRR v2016 CM:MIL2.Q4 CRR v2016 CM:MIL3.Q3 CRR v2016 CM:MIL4.Q3 CRR v2016 EDM:MIL2.Q3 CRR v2016 EDM:MIL3.Q3 CRR v2016 EDM:MIL5.Q2 CRR v2016 IM:MIL3.Q3

	CRR v2016 IM:MIL5.Q2 CRR v2016 RM:MIL2.Q3 CRR v2016 RM:MIL3.Q3 CRR v2016 RM:MIL5.Q2 CRR v2016 SA:G1.Q3 CRR v2016 SA:G2.Q1 CRR v2016 SA:G2.Q2 CRR v2016 SA:G3.Q1 CRR v2016 SA:G3.Q2 CRR v2016 SA:MIL2.Q3 CRR v2016 SA:MIL3.Q3 CRR v2016 SA:MIL5.Q2 CRR v2016 SCM:MIL2.Q3 CRR v2016 SCM:MIL3.Q3 CRR v2016 SCM:MIL5.Q2 CRR v2016 TA:MIL2.Q2 CRR v2016 TA:MIL2.Q3 CRR v2016 TA:MIL3.Q3 CRR v2016 TA:MIL5.Q2 CRR v2016 VM:MIL2.Q3 CRR v2016 VM:MIL3.Q3 CRR v2016 VM:MIL5.Q2 FedRAMP PL-2(3) FedRAMP SA-2 FFIEC IS v2016 A.1.5 FFIEC IS v2016 A.3.1c FFIEC IS v2016 A.8.1(n) IRS Pub 1075 v2016 9.3.15.2 MARS-E v2 PL-2(3) MARS-E v2 PM-1 MARS-E v2 PM-3 MARS-E v2 SA-2 NIST Cybersecurity Framework v1.1 ID.BE-3 NIST Cybersecurity Framework v1.1 ID.GV-2 NIST SP 800-53 R4 PM-11a[HML]{0} NIST SP 800-53 R4 SA-2[HML]{0} NY DOH SSP v3.1 PM-11a[M]-1 NY DOH SSP v3.1 PM-11a[M]-2 NY DOH SSP v3.1 PM-11b[M]-2 NY DOH SSP v3.1 SA-2a[M]-0 NY DOH SSP v3.1 SA-2b[M]-0 NY DOH SSP v3.1 SA-2c[M]-0 TJC IM.02.01.03, EP 8

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CMMC Level 2 Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to HIPAA Security Rule Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Basic Level

	Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: Information security coordination involves the active cooperation and collaboration across the entire organization to include managers, users, administrators, application designers, auditors, and security personnel. Information security coordination also includes specialist skills in areas such as insurance, legal issues, human resources, privacy, IT, or risk management. This activity: 1. addresses deviations via a risk acceptance process; 2. approves methodologies and processes for information security management activities (e.g., risk acceptance, information classification, security incidents); 3. identifies and promptly reports to senior management significant threat changes and exposure of information and information processing resources to threats; 4. evaluates information received from the monitoring and reviewing of information security incidents to conduct "lessons learned" activities and recommends to senior management appropriate actions in response to identified information security incidents. 5. creates an internal security information sharing mechanism, such as an email group, periodic conference call or standing meeting; and 6. establishes an internal reporting mechanism, such as a telephone hotline or dedicated email address, to allow security contacts to report information security incidents or obtain security policy clarifications on a timely basis. The organization develops a security plan for the information system that: 1. is consistent with the organization's enterprise architecture; 2. explicitly defines the authorization boundary for the system; 3. describes the operational context of the information system in terms of missions and business processes; 4. provides the security categorization of the information system including supporting rationale; 5. describes the operational environment for the information system; 6. describes relationships with, or connections to, other information systems; 7. provides an overview of the security requirements for the system; 8. identifies any relevant overlays, if applicable; 9. describes the security controls, in place or planned, for meeting those requirements including a rationale for tailoring and supplementation decisions; and 10. is reviewed and approved by the authorizing official or designated representative prior to plan implementation. The organization updates the system security plan: 1. at least every three years; 2. when substantial changes are made to the system; 3. when changes in requirements result in the need to process data of a higher sensitivity; 4. after the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and

	5. prior to expiration of a previous security authorization. The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on other organizational entities. The organization: 1. distributes copies of the information system's security plan to appropriate individuals and offices (e.g., CCO, CIO, business units); 2. communicates any changes to the security plans to appropriate individuals and offices; and 3. protects the plan from unauthorized disclosure and modification.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.316(b)(2)(iii) HIPAA.SR-3 AICPA 2017 CC2.2 AICPA 2017 CC3.4 CMMC v1.0 CA.2.157-1 CMMC v1.0 CA.2.157-4 CMSRs v3.1 PL-02 (HIGH; MOD) CMSRs v3.1 PL-02(03) (HIGH; MOD) CMSRs v3.1 PM-01 (HIGH; MOD) CRR v2016 AM:MIL2.Q3 CRR v2016 AM:MIL5.Q2 CRR v2016 CCM:MIL2.Q3 CRR v2016 CCM:MIL5.Q2 CRR v2016 CM:MIL2.Q3 CRR v2016 CM:MIL5.Q2 CRR v2016 EDM:MIL2.Q3 CRR v2016 EDM:MIL4.Q3 CRR v2016 EDM:MIL5.Q2 CRR v2016 IM:MIL4.Q3 CRR v2016 IM:MIL5.Q2 CRR v2016 RM:MIL2.Q3 CRR v2016 RM:MIL4.Q3 CRR v2016 RM:MIL5.Q2 CRR v2016 SA:MIL2.Q3 CRR v2016 SA:MIL4.Q3 CRR v2016 SA:MIL5.Q2 CRR v2016 SCM:MIL2.Q3 CRR v2016 SCM:MIL4.Q3 CRR v2016 SCM:MIL5.Q2 CRR v2016 TA:MIL2.Q3 CRR v2016 TA:MIL4.Q3 CRR v2016 TA:MIL5.Q2 CRR v2016 VM:MIL2.Q3 CRR v2016 VM:MIL4.Q3 CRR v2016 VM:MIL5.Q2 FedRAMP PL-2 FedRAMP PL-2(3) FFIEC IS v2016 A.1.5 FFIEC IS v2016 A.3.1 IRS Pub 1075 v2016 7.4 IRS Pub 1075 v2016 9.3.12.2 IRS Pub 1075 v2016 9.4.1 IRS Pub 1075 v2016 9.4.14 MARS-E v2 PL-2 MARS-E v2 PL-2(3) MARS-E v2 PM-1 NIST 800-171 r2 3.12.4-1 NIST 800-171 r2 3.12.4-4 NIST Cybersecurity Framework v1.1 DE.DP-4 NIST Cybersecurity Framework v1.1 ID.GV-2 NIST SP 800-53 R4 AC-17(6)[S]{1} NIST SP 800-53 R4 CA-2c[HML]{0} NIST SP 800-53 R4 CA-2d[HML]{0} NIST SP 800-53 R4 PL-2b[HML]{0} NIST SP 800-53 R4 PL-2e[HML]{0} NIST SP 800-53 R4 PM-6[HML]{0} NIST SP 800-53 R4 SI-5(1)[H]{0} NIST SP 800-53 R4 SI-6(2)[S]{0}

	NIST SP 800-53 R4 SI-6(3)[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 AC-3(9).NYS[MN]-1 NY DOH SSP v3.1 AC-5a[M]-2 NY DOH SSP v3.1 PL-2b[M]-0 NY DOH SSP v3.1 PL-2e[M]-0 NY DOH SSP v3.1 PM-16[M]-1 PCI DSS v3.2.1 12.5.2 PMI DSP Framework RC-3

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	
Level 3 Implementation:	Level 2 plus: The organization convenes an internal meeting for the organization's security single point of contact and the organizational area/business unit security contacts (see 05.a) on a monthly or near to monthly basis.
Level 3 Control Standard Mapping:	NIST Cybersecurity Framework v1.1 ID.GV-2 NIST Cybersecurity Framework v1.1 PR.IP-8

Level CMS Implementation Requirements

Level CMS Implementation:	The organization establishes a discrete line item in CMS' programming and budgeting documentation for the implementation and management of information systems security. The organization develops a security plan for the information system that is consistent with the CMS System Security Plan (SSP) Procedure.

Level DGF Implementation Requirements

Level DGF Implementation:	The stakeholders impacted by Data Governance are well understood. Funding for Data Governance activities are budgeted and provided for.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	Security plans are reviewed at least annually, when changes are made to the information system or information protection requirements, or when incidents occur that impact the plans' validity.

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation:	The organization develops and submits to designated agency officials and the Office of Safeguards a Safeguard Procedures Report (SPR) that describes the procedures established and used by the organization for ensuring the confidentiality of the information received from the IRS. Annually thereafter, the organization must file a Safeguard Activity Report (SAR). Whenever significant changes occur in the safeguard program the SPR will be updated and resubmitted to designated agency officials and the Office of Safeguards. It also advises the IRS of future actions that will affect the organization's current efforts to ensure the confidentiality of FTI and certifies that the organization is protecting FTI pursuant to IRC Section 6103(p)(4) and the organization's own security requirements. Agencies must notify the IRS prior to executing any agreement to disclose FTI to a contractor (e.g., cloud computing providers, consolidated data centers, off-site storage facilities, shred companies, information technology support, or tax modeling or revenue forecasting providers), or at least 45 days prior to the disclosure of FTI, to ensure that appropriate contractual language is included, and that contractors are held to safeguarding requirements. Further, any contractors authorized access to or possession of FTI must notify and secure the approval of the IRS prior to making any redisclosures to subcontractors. (See IRS Pub 1075 v2014 Exhibit 6.)

Level NYDOH Implementation Requirements	
Level NYDOH Implementation:	The organization develops a security plan for the information system that is consistent with (i) the RMH Procedures; and (ii) is consistent with the organization's enterprise architecture; (iii) explicitly defines the authorization boundary for the system; (iv) describes the operational context of the information system in terms of missions and business processes; (v) provides the security categorization of the information system including supporting rationale; (vi) describes the operational environment for the information system and relationships with or connections to other information systems; (vii) provides an overview of the security requirements for the system; (viii) identifies any relevant overlays, if applicable; (ix) describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and (x) is reviewed and approved by the authorizing official or designated representative prior to plan implementation. The organization updates the security plan, (i) minimally every three (3) years, to address current conditions or whenever (ii) there are significant changes to the information system/environment of operation that affect security; (iii) problems are identified during plan implementation or security control assessments; (iv) the data sensitivity level increases; (v) after a serious security violation due to changes in the threat environment; or (vi) before the previous security authorization expires. Systems processing, storing, or transmitting PII (to include PHI): The system security plan (SSP) must provide the security category and the personally identifiable information (PII) confidentiality impact level of the system (as described in NIST SP 800-122), describe relationships with, and data flows of, PII to other systems, and provide an overview of security and privacy requirements for the system; the SSP must define the boundary within the system where PII is stored, processed, and/or maintained; and the person responsible for meeting information system privacy requirements must provide input to the SSP. The organization plans and coordinates security-related activities affecting the information system with affected internal or external stakeholders, groups, or

	organizations before conducting such activities to reduce the impact on other organizational entities. Systems processing, storing, or transmitting PII (to include PHI): As part of the capital planning and investment control process, the organization must determine, document, and allocate resources required to protect the privacy and confidentiality of personally identifiable information (PII) in the information system. The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Control Reference: 05.c Allocation of Information Security Responsibilities

Control Specification:	All information security responsibilities shall be clearly defined.
Factor Type:	Organizational
Topics:	Authorization; IT Organization and Management Roles and Responsibilities; Media and Assets

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to HITRUST De-ID Framework Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to PCI Compliance Subject to Texas Health and Safety Code
Level 1 Implementation:	The organization's senior-level information security official coordinates, develops, implements, and maintains an organization-wide information security program. The organization formally assigns the following specific information security responsibilities to an individual or team: 1. establishment, documentation and distribution of security policies and procedures; 2. monitoring and analyzing security alerts and information, and distributing security alerts, information, and analysis to appropriate personnel; 3. establishment, documentation and distribution of security incident response and escalation procedures to ensure timely and effective handling of all situations; 4. administering user accounts, including additions, deletions, and modifications; and 5. monitoring and controlling all access to data. Information security roles and responsibilities are coordinated and aligned with internal roles and external partners. The organization clearly assigns responsibilities to identify all IT assets that need protection and apply controls to meet security policy. The allocation of information security responsibilities is done in accordance with the information security policy.

	Responsibilities for the protection of individual assets and for carrying out specific security processes are clearly identified. This responsibility is supplemented, where necessary, with more detailed guidance for specific assets and facilities. Individuals with allocated security responsibilities may delegate security tasks to others. Nevertheless, they remain accountable and are expected to determine that any delegated tasks have been correctly performed.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) AICPA 2017 CC5.3 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 PM-02 (HIGH; MOD) CMSRs v3.1 PM-10 (HIGH; MOD) COBIT 5 APO13.01 COBIT 5 APO13.02 COBIT 5 DS5.1 CRR v2016 SA:G1.Q1 CRR v2016 SA:MIL2.Q2 CSA CCM v3.0.1 GRM-04 CSA CCM v3.0.1 HRS-07 De-ID Framework v1 Accountable Individuals: General FFIEC IS v2016 A.1.5 FFIEC IS v2016 A.2.7 FFIEC IS v2016 A.2.8 FFIEC IS v2016 A.2.9 IRS Pub 1075 v2016 9.3.18.1 ISO/IEC 27002:2013 6.1.1 ISO/IEC 27799:2016 6.1.1 MARS-E v2 PM-10 MARS-E v2 PM-2 NIST Cybersecurity Framework v1.1 ID.GV-1 NIST Cybersecurity Framework v1.1 ID.GV-2 NIST SP 800-53 R4 PM-2[HML]{0} NIST SP 800-53 R4 SA-3c[HML]{0} NRS 603A.215.1 PCI DSS v3.2.1 12.4 PCI DSS v3.2.1 12.5 PCI DSS v3.2.1 12.5.1 PCI DSS v3.2.1 12.5.2 PCI DSS v3.2.1 12.5.3 PCI DSS v3.2.1 12.5.4 PCI DSS v3.2.1 12.5.5

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to FISMA Compliance Subject to FTC Red Flags Rule Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)

Level 2 Implementation:	Level 1 plus: The organization identifies by name or position non-professional or professional security contacts in each major organizational area or business unit. The organization clearly defines the roles, responsibilities and authority of each security contact including the administration and implementation of the organization's security programs. Each security contact annually documents compliance related to identified legal requirements (see CSF 06.a) and reports to the organization's single point of contact for security. The reports include: 1. evaluations on the effectiveness of the policies and procedures implemented in addressing risk; 2. evaluations of service provider arrangements (see CSF 09.e, 09.f, 09.g); 3. significant incidents and the response; and 4. recommendations for material changes to the security programs for which they are responsible. The organization's single point of contact for security matters provides supplemental security awareness and training. The contact for security is responsible for review reports related to the security organization, network, systems, and programs implemented. Any material changes to these items are formally approved by the contact for security prior to implementation. Local responsibilities for the protection of assets and for carrying out specific security processes, such as business continuity planning, are clearly defined. Additionally, the following takes place: 1. the assets and security processes associated with each particular system are identified and clearly defined; 2. the entity responsible (owner) for each asset or security process is assigned and the details of this responsibility are documented (see 07.b); 3. authorization levels are clearly defined and documented; and 4. to be able to fulfil responsibilities in the information security area, the appointed individuals are competent in the area and given opportunities to keep up to date with developments.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(3) 1 TAC § 390.2(a)(4)(A)(xi) 16 CFR Part § 681 Appendix A VI(a) 16 CFR Part § 681 Appendix A VI(b) AICPA 2017 CC1.3 CMSRs v3.1 AT-03 (HIGH; MOD) CMSRs v3.1 IR-02 (HIGH; MOD) CMSRs v3.1 PM-10 (HIGH; MOD) CSA CCM v3.0.1 HRS-07 FedRAMP AT-3 FFIEC IS v2016 A.1.5 FFIEC IS v2016 A.2.7 FFIEC IS v2016 A.2.8 FFIEC IS v2016 A.2.9 HITRUST IRS Pub 1075 v2016 9.3.2.3 IRS Pub 1075 v2016 9.3.8.2 ISO/IEC 27002:2013 6.1.1 ISO/IEC 27002:2013 6.1.3 ISO/IEC 27799:2016 6.1.3 MARS-E v2 AT-3 MARS-E v2 IR-2 MARS-E v2 PM-10 NIST Cybersecurity Framework v1.1 ID.GV-2 NIST Cybersecurity Framework v1.1 PR.AT-1 NIST Cybersecurity Framework v1.1 PR.AT-2

	NIST Cybersecurity Framework v1.1 PR.AT-4 NIST Cybersecurity Framework v1.1 PR.AT-5 NY DOH SSP v3.1 AC-5.IS2[M]-1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to FedRAMP Certification Subject to NY OHIP Moderate-Plus Security Baseline
Level 3 Implementation:	Level 2 plus: The organization specifically defines the roles, responsibilities of each security contact in writing.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 SA-03 (HIGH; MOD) CSA CCM v3.0.1 HRS-07 FedRAMP SA-3 IRS Pub 1075 v2016 9.3.15.3 ISO/IEC 27002:2013 6.1.1 ISO/IEC 27799:2016 6.1.1 MARS-E v2 SA-3 NIST Cybersecurity Framework v1.1 ID.GV-2 NIST Cybersecurity Framework v1.1 PR.AT-5 NY DOH SSP v3.1 SA-3c[M]-0

Level DGF Implementation Requirements

Level DGF Implementation:	The organization has identified an executive owner responsible for the Data Governance program, goals, and implementation roadmap.

Control Reference: 05.d Authorization Process for Information Assets and Facilities

Control Specification:	A management authorization process for new information assets (e.g., systems and applications) (see Other Information), and facilities (e.g., data centers or offices where covered information is to be processed) shall be defined and implemented.
Factor Type:	Organizational
Topics:	Authorization; IT Organization and Management Roles and Responsibilities; Media and Assets; Physical and Facility Security; Policies and Procedures; Requirements (Legal and Contractual)

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1	

System Factors:	
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Supplemental)
Level 1 Implementation:	The following are required for the authorization process: 1. new information processing assets (internal to the organization or via a service provided by a third-party) have appropriate user management authorization of their purpose and use, and authorization is also obtained from the manager responsible for maintaining the local information system security environment to ensure that all relevant security policies and requirements are met; 2. information assets have appropriate security measures commensurate with the type of information they will store, process, or transmit; 3. the assets comply with all applicable laws, regulations, standards policies, and other applicable sections of the HITRUST Common Security Framework; 4. hardware and software are checked to ensure that they are compatible with other system components; and 5. necessary controls for the use of personal or privately owned information processing equipment (e.g., laptops, home-computers, or hand-held devices) for processing business information, which may introduce new vulnerabilities, are identified, and implemented.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) CMSRs v3.1 PM-10 (HIGH; MOD) CRR v2016 AM:G5.Q1 MARS-E v2 PM-10 NIST Cybersecurity Framework v1.1 ID.BE-1 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST SP 800-53 R4 PE-20b[S]{1} NIST SP 800-53 R4 SA-13a[S]{1}

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to FISMA Compliance Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate)
Level 2 Implementation:	Level 1 plus: Management formally authorizes (approves) new information assets and facilities for processing (use) before commencing operations and periodically reviews and updates authorizations (approvals) at a frequency defined by the organization but no less than three years.
Level 2 Control Standard	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC6.1 CMSRs v3.1 CA-06 (HIGH; MOD)

Mapping:	FedRAMP CA-6 IRS Pub 1075 v2016 9.3.4.5 MARS-E v2 CA-6 NIST Cybersecurity Framework v1.1 ID.BE-1 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST SP 800-53 R4 CA-6[HML]{0}

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to CRR V2016 Subject to FedRAMP Certification Subject to NY OHIP Moderate-Plus Security Baseline
Level 3 Implementation:	Level 2 plus: All facilities undergo a site security survey, prior to lease or purchase, by the organization's security department or a trusted third-party, and resolve all security shortcomings before any covered information is processed at that location. All sites that process covered information are reviewed on an annual basis to ensure their continued suitability to process covered information. This process is also invoked if the site undergoes a significant change in mission or makes substantive physical changes in its facilities or workforce.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC3.4 AICPA 2017 CC8.1 CMSRs v3.1 CA-02 (HIGH; MOD) CMSRs v3.1 RA-03 (HIGH; MOD) CRR v2016 AM:G7.Q3 FedRAMP CA-2 FedRAMP RA-3 IRS Pub 1075 v2016 9.3.14.2 IRS Pub 1075 v2016 9.3.4.2 MARS-E v2 CA-2 MARS-E v2 RA-3 NIST Cybersecurity Framework v1.1 ID.BE-1 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 ID.RA-4 NY DOH SSP v3.1 CA-6a1[M]-2 NY DOH SSP v3.1 CA-6a2[M]-2 NY DOH SSP v3.1 CA-6a3[M]-2

Level CMS Implementation Requirements

Level CMS Implementation:	The organization: 1. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and 2. Updates the security authorization: i. Within every three years;

	ii. When significant changes are made to the system; iii. When changes in requirements result in the need to process data of a higher sensitivity; iv. When changes occur to authorizing legislation or federal requirements; v. After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and vi. Prior to expiration of a previous security authorization.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	Owners of FTI accredit the security controls used to protect FTI before initiating operations. This is done for any infrastructure associated with FTI. The authorization occurs every three years or whenever there is a significant change to the control structure. A senior agency official signs and approves the authorization.

Level HIX Implementation Requirements

Level HIX Implementation:	The organization ensures that the authorizing official authorizes the information system for processing before commencing operations, and a senior organization official signs. The systems Authority to Operate (ATO) and, if the organization maintains a system-to-system connection with CMS through an executed interconnection security agreement (ISA), the CMS-granted Authority to Connect (ATC) is updated (i) within every three years; (ii) when significant changes are made to the system; (iii) when changes in requirements result in the need to process data of a higher sensitivity; (iv) when changes occur to authorizing legislation or federal requirements; (v) after the occurrence of a serious security violation, which raises questions about the validity of an earlier security authorization; and (vi) prior to the expiration of a previous security authorization.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The CMS CIO, CISO, and Senior Official for Privacy (SOP) have the authority to order the immediate termination and/or suspension of any interconnection that, in the judgment of the CMS officer and CMS Security Operations, presents an unacceptable level of risk to the CMS enterprise and/or mission. The organization updates the security authorization when changes occur to authorizing legislation or federal requirements that impact the system. The organization updates the security authorization after the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization. The organization updates the security authorization prior to expiration of a previous security authorization. The organization (i) manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes; (ii) designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and (iii) fully integrates the security authorization processes into an organization-wide risk management program.

Control Reference: 05.e Confidentiality Agreements

Control Specification:	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed.
Factor Type:	Organizational
Topics:	Documentation and Records; Personnel; Requirements (Legal and Contractual); Third-parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Supplemental)
Level 1 Implementation:	Confidentiality or non-disclosure agreements address the requirement to protect confidential information using legally enforceable terms. Confidentiality or non-disclosure agreements include, but are not limited to, the following: 1. a definition of the information to be protected (e.g., confidential information); 2. expected duration of an agreement, including cases where confidentiality might need to be maintained indefinitely; 3. required actions when an agreement is terminated; 4. responsibilities and actions of signatories to avoid unauthorized information disclosure (such as 'need to know'); 5. disclosures required to be limited to the limited data set (see 07.d) or the minimum necessary to accomplish the intended purpose of such use, disclosure, or request; 6. ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information; 7. the permitted use of confidential information, and rights of the signatory to use information; 8. individuals' rights to obtain a copy of the individual's information in an electronic format; 9. individuals' rights to have the individual's information transmitted to another entity or person designated by the individual, provided the request is clear, conspicuous, and specific; 10. the right to audit and monitor activities that involve confidential information; 11. the process for notification and reporting of unauthorized disclosure or confidential information breaches; 12. terms for information to be returned or destroyed at agreement cessation; and 13. expected actions to be taken (i.e., penalties that are possible) in case of a breach of this agreement. The confidentiality agreement is applicable to all personnel accessing covered information. Confidentiality and non-disclosure agreements comply with all applicable laws and regulations for the jurisdiction to which it applies (see 6.a). Requirements for confidentiality and non-disclosure agreements are reviewed at least annually and when changes occur that influence these requirements.
Level 1 Control Standard Mapping:	CSA CCM v3.0.1 HRS-06 FFIEC IS v2016 A.6.31(d) FFIEC IS v2016 A.6.8(e) ISO/IEC 27002:2013 13.2.4 ISO/IEC 27799:2016 13.2.4 NIST Cybersecurity Framework v1.1 ID.GV-3

	NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 AC-19(4)b[S]{4} NIST SP 800-53 R4 PS-6(2)c[S]{1} PMI DSP Framework RS-1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	
Level 2 Implementation:	Level 1 plus: The organization publishes a list of representatives who are authorized to sign a non-disclosure agreement on behalf of the organization. This list is kept up to date to reflect personnel changes and departures.
Level 2 Control Standard Mapping:	HITRUST NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 PR.DS-5

Level HIE Implementation Requirements

Level HIE Implementation:	As part of the agreement with the connecting organizations, the HIE specifies which organization owns the data and any restrictions as part of that ownership such as retention, integrity, and accuracy of data. If the HIE is the owner of the data, all federal and state requirements associated with the patients' information is met.

Control Reference: 05.f Contact with Authorities

Control Specification:	Appropriate contacts with relevant authorities shall be maintained.
Factor Type:	Organizational
Topics:	Documentation and Records; Incident Response; Policies and Procedures; Third-parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1	

Regulatory Factors:	
Level 1 Implementation:	The organization defines a plan with associated contact information for reporting security incidents to law enforcement if it is suspected that laws may have been broken. The organization includes key contacts including phone numbers and email addresses as part of its incident management and/or business continuity plan. The organization designates a point of contact to review the list at least annually to keep it current. Organizations under attack from the Internet may need external third-parties (e.g., an Internet service provider or telecommunications operator) to take action against the attack source. The appropriate contact information for these third-parties is documented, and instances when they must be contacted to take action are communicated.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 CP-02 (HIGH; MOD) CSA CCM v3.0.1 SEF-01 FedRAMP CP-2 FFIEC IS v2016 A.8.1(f) IRS Pub 1075 v2016 9.3.6.2 ISO/IEC 27002:2013 6.1.3 ISO/IEC 27799:2016 6.1.3 MARS-E v2 CP-2 NIST Cybersecurity Framework v1.1 DE.DP-4 NIST Cybersecurity Framework v1.1 RS.CO-2 NIST Cybersecurity Framework v1.1 RS.CO-3 PMI DSP Framework RS-1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CRR V2016 Subject to FedRAMP Certification
Level 2 Implementation:	Level 1 plus: Each group within the organization (e.g., information security) has procedures documented and implemented that specify when, and by whom, authorities (e.g., law enforcement, fire department, supervisory authorities) are contacted, and how identified information security incidents are reported in a timely manner if it is suspected that laws may have been broken. The organization includes key contacts including phone numbers and email addresses as part of its incident management and/or business continuity plan. The organization designates a point of contact to review the list at least quarterly to keep it current. The organization conducts an exercise at least annually and make contact with a majority (at least 80%) of the listed contacts. During this incident/continuity plan

	exercise, the organization documents that the contact person and information are current.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC7.3 CMSRs v3.1 CP-02 (HIGH; MOD) CMSRs v3.1 CP-04 (HIGH; MOD) CRR v2016 EDM:G5.Q1 CSA CCM v3.0.1 SEF-01 FedRAMP CP-2 FedRAMP CP-4 FedRAMP IR-6 FFIEC IS v2016 A.8.1(f) IRS Pub 1075 v2016 9.3.6.2 IRS Pub 1075 v2016 9.3.6.4 ISO/IEC 27002:2013 6.1.3 ISO/IEC 27002:2013 6.1.6 ISO/IEC 27799:2016 6.1.3 ISO/IEC 27799:2016 6.1.6 MARS-E v2 CP-2 MARS-E v2 CP-4 NIST Cybersecurity Framework v1.1 DE.DP-4 NIST Cybersecurity Framework v1.1 RS.CO-2 NIST Cybersecurity Framework v1.1 RS.CO-3

Control Reference: 05.g Contact with Special Interest Groups

Control Specification:	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
Factor Type:	Organizational
Topics:	Incident Response; Third-parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline
Level 1 Implementation:	Membership in organization-defined special interest groups or forums/services (e.g., threat monitoring/intelligence services, security researchers) is considered as a means to: 1. improve knowledge about best practices and staying up to date with relevant security information; 2. ensure the understanding of the information security environment is current and complete; 3. receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities; 4. gain access to specialist information security advice; 5. share and exchange information about new technologies, products, threats, or vulnerabilities; 6. provide suitable liaison points when dealing with information security incidents (see 11.c).

Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 PM-15 (HIGH; MOD) CRR v2016 SA:G1.Q2 CSA CCM v3.0.1 SEF-01 FFIEC IS v2016 A.4.3 FFIEC IS v2016 A.4.4 IRS Pub 1075 v2016 9.3.17.5 ISO/IEC 27002:2013 6.1.4 ISO/IEC 27799:2016 6.1.4 MARS-E v2 PM-15 NIST Cybersecurity Framework v1.1 ID.RA-2 NIST Cybersecurity Framework v1.1 RS.CO-5 NIST SP 800-53 R4 IR-4(8)[S]{2} NIST SP 800-53 R4 PM-15[HML]{0} NIST SP 800-53 R4 PM-16[HML]{0} NY DOH SSP v3.1 PM-15a[M]-2 NY DOH SSP v3.1 PM-15b[M]-0 PMI DSP Framework DE-4

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CMMC Level 2 Subject to CMMC Level 3 Subject to CMMC Level 4 Subject to CRR V2016 Subject to FISMA Compliance Subject to HIPAA Security Rule Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Basic Level Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Supplemental Requirements Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: Membership in special interest groups or forums/services is required and actively maintained. The organization has a process to quickly identify newly discovered security threats and vulnerabilities such as a credible subscription service. The organization has a process to map new threats and vulnerabilities into its security policies, guidelines, and daily operational procedures.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.308(a)(5)(ii)(A) HIPAA.SR-2 CMMC v1.0 IR.4.100-1 CMMC v1.0 SA.3.169-1

	CMMC v1.0 SA.3.169-2 CMMC v1.0 SI.2.214-0 CMSRs v3.1 PM-15 (HIGH; MOD) CMSRs v3.1 SI-05 (HIGH; MOD) CMSRs v3.1 SI-05(01) (HIGH) CRR v2016 SA:G1.Q2 FFIEC IS v2016 A.4.3 FFIEC IS v2016 A.4.4 IRS Pub 1075 v2016 9.3.17.5 ISO/IEC 27002:2013 6.1.4 ISO/IEC 27799:2016 6.1.4 MARS-E v2 PM-15 MARS-E v2 SI-5 NIST 800-171 r2 3.14.3-0 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 ID.RA-2 NIST Cybersecurity Framework v1.1 RS.AN-5 NIST Cybersecurity Framework v1.1 RS.CO-3 NIST Cybersecurity Framework v1.1 RS.CO-5 NIST SP 800-53 R4 IR-4(8)[S]{1} NY DOH SSP v3.1 PM-15a[M]-3 PMI DSP Framework DE-4 SR v6.4 1-0

Level CMS Implementation Requirements

Level CMS Implementation:	The organization implements security directives in accordance with established time frames or notifies CMS of the degree of noncompliance. The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The organization receives information system security alerts, advisories, and directives from US-CERT on an ongoing basis. Further the organization generates and disseminates security alerts, advisories, and directives to organization-defined personnel with roles in system administration, monitoring, and/or security responsibilities, and implements security directives in accordance with established time frames or notifies the business owner of the degree of noncompliance.

Level HIX Implementation Requirements

Level HIX Implementation:	The organization disseminates security alerts, advisories, and directives to organization-defined personnel with roles in system administration, monitoring, and/or security responsibilities, and implements security directives in accordance with established time frames or notifies the business owner of the degree of noncompliance.

Control Reference: 05.h Independent Review of Information Security

Control Specification:	The organization's approach to managing information security and its implementation (control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, at a minimum annually, or when significant changes to the security implementation occur. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational

Topics:	Audit and Accountability; Documentation and Records; IT Organization and Management Roles and Responsibilities

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to Texas Health and Safety Code Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	An independent review of the organization's information security management program is initiated by management. Such an independent review is necessary to ensure the continuing suitability, adequacy, and effectiveness of the organization's approach to managing information security and privacy. The review: 1. includes an assessment of the organization's adherence to its security plan and the tests and methods used is sufficient to validate the effectiveness of the security plan; 2. includes notification requirements to confirm whom to inform within the organization about the timing and nature of the assessment; 3. addresses the need for changes to the approach to security in light of evolving circumstances, including the policy and control objectives and other opportunities for improvement, including those based on regular vulnerability assessments (e.g., network scans and penetration testing); 4. carefully controls information security tests to limit the risks to confidentiality, integrity, and system availability; 5. is carried out by individuals independent of the area under review (e.g., the internal audit function, an independent manager or a third-party organization specializing in such reviews); and 6. is carried out by individuals who have the appropriate skills and experience. The results of the independent review: 1. are recorded and reported to the management who initiated the review; and 2. are maintained for a predetermined period of time as determined by the organization, but not less than three years. If the independent review identifies that the organization's approach and implementation to managing information security is inadequate or not compliant with the direction for information security stated in the information security policy document (see 4.a), management takes corrective actions.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 201 CMR 17.03(2)(b) AICPA 2017 CC4.2 AICPA 2017 P8.1 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 AR-04 (HIGH) CMSRs v3.1 AR-04 (HIGH; MOD) CMSRs v3.1 CA-02 (HIGH; MOD) CMSRs v3.1 CA-02(01) (HIGH; MOD) CMSRs v3.1 CA-07 (HIGH; MOD) CMSRs v3.1 CA-07(01) (HIGH; MOD)

	COBIT 5 DS5.5 COBIT 5 DSS05.07 CRR v2016 VM:MIL4.Q1 CSA CCM v3.0.1 AAC-02 De-ID Framework v1 Privacy Reviews/Audits: General FedRAMP CA-2 FedRAMP CA-2(1) FedRAMP CA-7 FedRAMP CA-7(1) FFIEC IS v2016 A.10.1 FFIEC IS v2016 A.10.3(d) FFIEC IS v2016 A.10.5 FFIEC IS v2016 A.10.6 FFIEC IS v2016 A.2.1(a) FFIEC IS v2016 A.2.1(b) FFIEC IS v2016 A.2.1(c) FFIEC IS v2016 A.6.8(c) FFIEC IS v2016 A.8.1(c) FFIEC IS v2016 A.9.1 FFIEC IS v2016 A.9.4 IRS Pub 1075 v2016 9.3.4.2 IRS Pub 1075 v2016 9.3.4.6 ISO/IEC 27002:2013 18.2.1 ISO/IEC 27799:2016 18.2.1 MARS-E v2 AR-4 MARS-E v2 CA-2 MARS-E v2 CA-2(1) MARS-E v2 CA-7 MARS-E v2 CA-7(1) NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 ID.RM-1 NIST Cybersecurity Framework v1.1 ID.RM-2 NIST Cybersecurity Framework v1.1 ID.RM-3 NIST Cybersecurity Framework v1.1 PR.IP-7 NIST Cybersecurity Framework v1.1 PR.IP-8 PMI DSP Framework ID-3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to FedRAMP Certification Subject to HIPAA Security Rule Subject to HITRUST De-ID Framework Requirements Subject to State of Massachusetts Data Protection Act
Level 2 Implementation:	Level 1 plus: The independent review of the information security management program and information security controls is conducted at least annually or whenever there is a material change to the business practices that may implicate the security or integrity of records containing personal information.

Level 2 Control Standard Mapping:	201 CMR 17.03(2)(a) 201 CMR 17.03(2)(b) 45 CFR Part § 164.308(a)(8) HIPAA.SR-0 AICPA 2017 CC3.4 CMSRs v3.1 CA-02 (HIGH; MOD) CMSRs v3.1 CA-02(01) (HIGH; MOD) De-ID Framework v1 Privacy Reviews/Audits: General FedRAMP CA-2 FFIEC IS v2016 A.10.1 FFIEC IS v2016 A.10.3(d) FFIEC IS v2016 A.10.6 FFIEC IS v2016 A.8.1(c) FFIEC IS v2016 A.9.1 FFIEC IS v2016 A.9.4 ISO/IEC 27002:2013 18.2.1 ISO/IEC 27799:2016 18.2.1 MARS-E v2 CA-2 MARS-E v2 CA-2(1) NIST Cybersecurity Framework v1.1 ID.GV-4

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The organization develops an information security and privacy control assessment plan that describes the scope of the assessment including: (i) security and privacy controls and control enhancements under assessment (including information security and privacy changes enacted by HHS and CMS CIO/CISO directives), (ii) assessment procedures to be used to determine control effectiveness and (iii) assessment environment, assessment team, and assessment roles and responsibilities. The organization assesses the security and privacy controls in the information system and its environment of operation, as defined in implementation standards, within every three hundred sixty-five [365] days in accordance with the CMS Information Security (IS) Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements (CMSR) Standard to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements. The organization provides the results of the security and privacy control assessment within thirty [30] days after its completion, in writing, to the Business Owner responsible for the system and personnel responsible for reviewing the assessment documentation and updating system security documentation where necessary to reflect any changes to the system. An assessment of all controls must be conducted prior to issuing the initial authority to operate for all newly implemented systems. When selected, penetration tests are performed when new risks and threats potentially affecting the system/applications are identified and reported or upon request from CMS.

Objective Name: 05.02 External Parties

Control Objective:	To ensure that the security of the organization's information and information assets, are not reduced by the introduction of external party products or services.

Control Reference: 05.i Identification of Risks Related to External Parties

Control Specification:	The risks to the organization's information and information assets from business processes involving external parties shall be identified, and appropriate controls implemented before granting access. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Authorization; Communications and Transmissions; Requirements (Legal and Contractual); Risk Management and Assessments; Third-parties and Contractors; User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to FTC Red Flags Rule Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (Supplemental) Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	Due diligence, including an evaluation of the information security risks posed by external parties, is carried out to identify any requirements for specific controls where access to sensitive information (e.g., covered information, cardholder data) by external parties is required prior to establishing a formal relationship with the service provider. The identification of risks related to external party access takes into account the following issues: 1. the information asset(s) an external party is required to access; 2. the type of access the external party will have to the information and information asset(s), such as: i. physical access (e.g., to offices, computer rooms, filing cabinets); ii. logical access (e.g., to an organization's databases, information systems); iii. network connectivity between the organization's and the external party's network(s) (e.g., permanent connection, remote access); and iv. whether the access is taking place on-site or off-site; 3. the value and sensitivity of the information involved, and its criticality for business operations; 4. the controls necessary to protect information that is not intended to be accessible by external parties; 5. the external party personnel involved in handling the organization's information; 6. how the organization or personnel authorized to have access can be identified, the authorization verified, and how often this needs to be reconfirmed; 7. the different means and controls employed by the external party when storing, processing, communicating, sharing, and exchanging information; 8. the impact of access not being available to the external party when required, and the external party entering or receiving inaccurate or misleading information; 9. practices and procedures to deal with information security incidents and potential damages, and the terms and conditions for the continuation of external party access in the case of an information security incident; 10. legal and regulatory requirements and other contractual obligations relevant to the external party that are taken into account;

	11. how the interests of any other stakeholders may be affected by the arrangements. Access by external parties to the organization's information is not provided until the appropriate controls have been implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement. All security requirements resulting from work with external parties or internal controls are reflected by the agreement with the external party (see 5.i and 5.j). All remote access connections between the organization and all external parties are secured via encrypted channels (e.g., VPN). Any covered information shared with an external party is encrypted prior to transmission. External parties are granted minimum necessary access to the organization's information assets to minimize risks to security. All access granted to external parties is limited in duration and revoked when no longer needed. It is ensured that the external party is aware of their obligations, and accepts the responsibilities and liabilities involved in accessing, processing, communicating, or managing the organization's information and information assets.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(3) 1 TAC § 390.2(a)(4)(A)(xi) 16 CFR Part § 681.1 (e)(4) AICPA 2017 CC2.3 CMSRs v3.1 AC-06 (HIGH; MOD) CMSRs v3.1 AC-17(02) (HIGH; MOD) CMSRs v3.1 CA-03 (HIGH; MOD) CMSRs v3.1 MA-04 (HIGH; MOD) CMSRs v3.1 SC-08(01) (HIGH; MOD) CRR v2016 CCM:G1.Q5 CRR v2016 CCM:G2.Q11 CRR v2016 EDM:G1.Q3 CRR v2016 EDM:G2.Q1 CRR v2016 EDM:MIL2.Q1 CRR v2016 EDM:MIL2.Q4 CSA CCM v3.0.1 IAM-07 CSA CCM v3.0.1 STA-05 EU GDPR Article 32(4) FedRAMP AC-17(2) FedRAMP AC-6 FedRAMP CA-3 FedRAMP MA-4 FFIEC IS v2016 A.3.3 FFIEC IS v2016 A.6.18(c) FFIEC IS v2016 A.6.23 FFIEC IS v2016 A.6.31(a) FFIEC IS v2016 A.6.31(b) FFIEC IS v2016 A.6.31(c) FFIEC IS v2016 A.6.31(f) FFIEC IS v2016 A.6.31(g) FFIEC IS v2016 A.6.7(a) FFIEC IS v2016 A.6.7(d) IRS Pub 1075 v2016 9.3.1.12 IRS Pub 1075 v2016 9.3.1.6 IRS Pub 1075 v2016 9.3.16.6 IRS Pub 1075 v2016 9.3.4.3 IRS Pub 1075 v2016 9.3.9.4 ISO/IEC 27002:2013 15.1.1 ISO/IEC 27002:2013 15.1.2 ISO/IEC 27002:2013 15.1.3 ISO/IEC 27799:2016 15.1.1 ISO/IEC 27799:2016 15.1.2 ISO/IEC 27799:2016 15.1.3 MARS-E v2 AC-17(2) MARS-E v2 AC-6 MARS-E v2 CA-3 MARS-E v2 MA-4 MARS-E v2 SC-8(1) NIST Cybersecurity Framework v1.1 DE.AE-1

	NIST Cybersecurity Framework v1.1 ID.AM-3 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 ID.RM-1 NIST Cybersecurity Framework v1.1 ID.RM-2 NIST Cybersecurity Framework v1.1 PR.AC-3 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.AT-3 NIST Cybersecurity Framework v1.1 PR.DS-2 NIST SP 800-53 R4 SA-14[S]{1} NRS 603A.215.1 PCI DSS v3.2.1 12.8.3 PMI DSP Framework ID-4 PMI DSP Framework PR.DS-4

Level 2	Implementation Requirements
Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to 23 NYCRR 500 Subject to Banking Requirements Subject to CMMC Level 4
Level 2 Implementation:	Level 1 plus: The organization conducts due diligence of the external party via interviews, document review, checklists, review certifications (e.g., HITRUST) or other remote means. The process for conducting external party due diligence is integrated with the execution of a non-disclosure agreement (NDA) (see 05.e). Organizations obtain satisfactory assurances that reasonable information security exists across their information supply chain by performing an annual review, which includes all partners/third-party providers upon which their information supply chain depends.
Level 2 Control Standard Mapping:	AICPA 2017 CC9.2 AICPA 2017 P6.1 AICPA 2017 P6.4 CMMC v1.0 RM.4.148-2 CSA CCM v3.0.1 STA-01 CSA CCM v3.0.1 STA-08 FFIEC IS v2016 A.3.3 FFIEC IS v2016 A.6.18(c) FFIEC IS v2016 A.6.31(b) FFIEC IS v2016 A.6.31(d) FFIEC IS v2016 A.6.31(e) NIST Cybersecurity Framework v1.1 ID.RM-1 NRS 603A.215.1 PCI DSS v3.2.1 12.8.3 PCI DSS v3.2.1 2.6

Level Cloud Service Providers	Implementation Requirements
Level Cloud Service Providers Implementation:	Providers inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers design and implement controls to

	mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.

Level Community Supplemental Reqs 02	Implementation Requirements
Level Community Supplemental Reqs 02 Implementation:	The organization performs due diligence on incident management service providers to ensure the provider has a credible history and is capable of providing the necessary services and re-evaluates the capabilities on a regular basis (e.g., prior to contract renewal).

Level FedRAMP	Implementation Requirements
Level FedRAMP Implementation:	The organization takes additional actions (e.g., requiring background checks for selected service provider personnel, examining ownership records, employing only providers for which it has had positive experiences, and conducting periodic/unscheduled visits to service provider facilities to ensure that the interests of external service providers for systems processing or storing covered information are consistent with and reflect organizational interests.

Level FFIEC IS	Implementation Requirements
Level FFIEC IS Implementation:	The organization identifies factors that increase the risk from supply chain attacks and respond with the following risk mitigations: 1. Purchases are made only through reputable vendors who demonstrate an ability to control their own supply chains; 2. Hardware is reviewed for anomalies; 3. Software is reviewed through both automated software testing and code reviews; and 4. Regularly reviewing the reliability of software and hardware items purchased through activity monitoring and evaluations by user groups. If the organization outsources cloud computing or storage to a third-party service provider, the organization addresses the key elements of outsourced cloud computing implementation and risk management in accordance with the FFIEC ISs Outsourced Cloud Computing statement. If the organization outsources management of security services to a third-party service provider, the organization addresses the key elements of outsourced security services implementation and risk management in accordance with appendix D of the FFIEC IS's IT Handbook "Outsourcing Technology Services" booklet.

Level NYDOH	Implementation Requirements
Level NYDOH Implementation:	Privacy requirements must be addressed in agreements that cover relationships in which external information systems are used to access, process, store, or transmit and manage PII. The organization facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for approved information-sharing circumstances where user discretion is required.

Control Reference: 05.j Addressing Security When Dealing with Customers

Control Specification:	All identified security requirements shall be addressed before giving customers access to the organization's information or assets. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Authentication; Incident Response; Requirements (Legal and Contractual); Third-parties and Contractors; User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to HITRUST De-ID Framework Requirements Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (Privacy) Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	The following security terms are addressed prior to giving customers access to any of the organization's assets: 1. description of the product or service to be provided; 2. the right to monitor, and revoke, any activity related to the organization's assets; and 3. the respective liabilities of the organization and the customer. It is ensured that the customer is aware of their obligations and rights, and accepts the responsibilities and liabilities prior to accessing, processing, communicating, or managing the organization's information and information assets. Awareness is provided through security awareness materials and education on an ongoing basis and discusses, at a minimum, how data will be used, the protections provided for their data (at a high-level), and any tools available to them to protect their own data. The organization permits an individual to request to restrict the disclosure of the individual's covered information to a business associate for purposes of carrying out payment or healthcare operations, and not for purposes of carrying out treatment. The organization responds to any requests from an individual on the disclosure of the individual's covered information, providing the individual with records (see 06.c) of disclosures of covered information that are made by the organization, and either: 1. records (see 06.c) of disclosures of covered information made by a business associate acting on behalf of the organization; or 2. a list of all business associates acting on behalf of the covered entity, including contact information for such associates (such as mailing address, phone, and email address). The organization ensures that the public has access to information about its security and privacy activities and is able to communicate with its senior privacy official (e.g., Chief Privacy Officer, Chief Data Protection Officer) senior security official (e.g., Chief Information Security Officer, Chief Data Protection Officer). Information may be provided

	on the organization's privacy and security program(s) (e.g., see 0.1, 03.a, 04.a, 06.d) at a high level; however, such information must, at a minimum, address the organization's privacy practices as required by statute (see 13.a) and describe the organization's breach notification process (see 11.a), actions individuals take to protect themselves (see 05.j), and how the public can easily submit information about potential vulnerabilities and bugs (see also 11.a).
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 PL-04 (HIGH; MOD) CMSRs v3.1 TR-03 (HIGH; MOD) CRR v2016 EDM:MIL2.Q4 CSA CCM v3.0.1 AIS-02 De-ID Framework v1 Transparency: General FedRAMP PL-4 IRS Pub 1075 v2016 9.3.12.3 IRS Pub 1075 v2016 9.4.13 IRS Pub 1075 v2016 9.4.16 IRS Pub 1075 v2016 9.4.5 MARS-E v2 PL-4 MARS-E v2 TR-3 NIST Cybersecurity Framework v1.1 PR.AT-3 NIST SP 800-53 R4 TR-3a[P]{0} PMI DSP Framework PR.AT-1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to FedRAMP Certification
Level 2 Implementation:	Level 1 plus: The following security terms are addressed prior to giving customers access to any of the organization's assets: 1. asset protection, including: i. procedures to protect the organization's assets, including information and software, and management of known vulnerabilities; ii. procedures to determine whether any compromise of the assets (e.g., loss or modification of data) has occurred; iii. integrity; and iv. restrictions on copying and disclosing information; 2. access control policy, covering: i. permitted access methods, and the control and use of unique identifiers such as user IDs and passwords; ii. an authorization process for user access and privileges; iii. a statement that all access that is not explicitly authorized is forbidden; iv. a process for revoking access rights or interrupting the connection between systems;

	3. arrangements for reporting, notification, and investigation of information inaccuracies (e.g., of personal details), information security incidents and security breaches; 4. a description of each service to be made available; 5. the target level of service and unacceptable levels of service; 6. the different reasons, requirements, and benefits for customer access; 7. responsibilities with respect to legal matters and how it is ensured that the legal requirements are met (e.g., data protection legislation), especially taking into account different national legal systems if the agreement involves co-operation with customers in other countries (see 06.i); and 8. intellectual property rights (IPRs) and copyright assignment (see 06.b) and protection of any collaborative work (see 05.e). Access by customers to the organization's information is not provided until the appropriate controls have been implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement. All security requirements resulting from work with external parties or internal controls are reflected by the agreement with the external party. For all system connections that allow customers to access the organization's computing assets such as websites, kiosks and public access terminals, the organization provides appropriate text or a link to the organization's privacy policy for data use and protection as well as the customer's responsibilities when accessing the data. The organization has a formal mechanism to authenticate (see 01.b) the customer's identity prior to granting access to covered information.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 AC-08 (HIGH; MOD) CMSRs v3.1 CA-03 (HIGH; MOD) CMSRs v3.1 TR-03 (HIGH; MOD) FedRAMP AC-8 FedRAMP CA-3 IRS Pub 1075 v2016 9.3.1.8 IRS Pub 1075 v2016 9.3.4.3 ISO/IEC 27002:2013 14.1.2 ISO/IEC 27799:2016 14.1.2 MARS-E v2 AC-8 MARS-E v2 CA-3 MARS-E v2 TR-3 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.AC-3 NIST Cybersecurity Framework v1.1 PR.AT-3 PMI DSP Framework PR.AC-1 PMI DSP Framework RS-1

Level FFIEC IS Implementation Requirements

Level FFIEC IS Implementation:	The organization provides secure customer access to financial services and develops and maintains policies and procedures to securely offer and ensure the resilience of remote financial services (e.g., using appropriate authentication, layered security controls, and fraud detection monitoring) in accordance with appendix E of the FFIEC IS's IT Handbook "Retail Payment Systems" booklet. The organization implements a customer awareness and education program that addresses both retail (consumer) and commercial account holders that addresses the following elements: 1. An explanation of protections provided, and not provided, to account holders relative to electronic funds transfers under Regulation E, and a related explanation of the applicability of Regulation E to the types of accounts accessible online;

	2. An explanation that while the institution may contact a customer regarding his or her account or suspicious activities related to his or her account, the institution never asks the customer to provide his or her log-in credentials over the phone or via e-mail; 3. A list of recommended controls and prudent practices that the customer implements when using the institutions remote financial services; 4. A suggestion that commercial online customers perform a related risk assessment and controls evaluation periodically; 5. Recommendations of technical and business controls to commercial customers that can be implemented to mitigate the risks from fraud schemes such as Business Email Compromise; and 6. A method to contact the institution if customers notice suspicious account activity.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	To use (i) an Integrated Voice Response (IVR) system that provides FTI over the telephone to a customer, or (ii) a web-based system or website to access FTI, the agency must ensure access to FTI via the IVR system requires a strong identity verification process. The authentication must use a minimum of two pieces of information although more than two are recommended to verify the identity. One of the authentication elements must be a shared secret only known to the parties involved and issued by the agency directly to the customer (but not a case number or similar piece of information). The organization's access control system must be specifically configured to address the complicated nature of the environment to ensure only authorized clients who conform to agency security policy are permitted access to the Virtual Desktop Infrastructure (VDI).

Level HIPAA Implementation Requirements

Level HIPAA Implementation:	The organization permits an individual to request to restrict the disclosure of the individual's covered information to a business associate for purposes of carrying out payment or healthcare operations, and not for purposes of carrying out treatment. The organization responds to any requests from an individual on the disclosure of the individual's covered information, providing the individual with records (see 06.c) of disclosures of covered information that are made by the organization, and either: 1. records (see 06.c) of disclosures of covered information made by a business associate acting on behalf of the organization; or 2. a list of all business associates acting on behalf of the covered entity, including contact information for such associates (such as mailing address, phone, and email address).

Control Reference: 05.k Addressing Security in Third Party Agreements

Control Specification:	Agreements with third-parties involving accessing, processing, communicating, or managing the organization's information or information assets, or adding products or services to information assets shall cover all relevant security requirements. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational

Topics:	Authorization; Awareness and Training; Documentation and Records; IT Organization and Management Roles and Responsibilities; Policies and Procedures; Requirements (Legal and Contractual); Third-parties and Contractors; User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 4 Subject to FISMA Compliance Subject to HIPAA Breach Notification Subject to HIPAA Security Rule Subject to HITRUST De-ID Framework Requirements Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to State of Massachusetts Data Protection Act Subject to Texas Health and Safety Code Subject to the CMS Minimum Security Requirements (High) Subject to the State of Nevada Security of Personal Information Requirements
Level 1 Implementation:	The organization identifies and mandates information security controls to specifically address supplier access to the organization's information and information assets. The organization maintains written agreements (contracts) that include an acknowledgement that the third-party (e.g., a service provider) is responsible for the security of the data the third-party possesses or otherwise stores, processes, or transmits on behalf of the organization, or to the extent that they could impact the security of the organization's information environment. Agreements include requirements to address the information security risks associated with information and communications technology services (e.g., cloud computing services) and product supply chain, and these requirements are subsequently applicable to subcontractors, etc., of the third-party, i.e., fourth parties, and so on throughout the supply chain. The agreement ensures that there is no misunderstanding between the organization and the third-party. Organizations satisfy themselves as to the indemnity of the third-party. The following terms are implemented for inclusion in the agreement in order to satisfy the identified security requirements (see 05.i): 1. the information security policy; 2. controls to ensure asset protection, including: i. procedures to protect organizational assets, including information, software, and hardware; ii. any required physical protection controls and mechanisms; iii. controls to ensure protection against malicious software (see 9.j); iv. procedures to determine whether any compromise of the assets (e.g., loss or modification of information, software, and hardware) has occurred; v. controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time, during the agreement; vi. confidentiality, integrity, availability, and any other relevant property of the assets; and

vii. restrictions on copying and disclosing information, and using confidentiality agreements (see 05.b);

3. user and administrator training in methods, procedures, and security;
4. ensuring user awareness for information security responsibilities and issues;
5. provision for the transfer of personnel, where appropriate;
6. responsibilities regarding hardware and software installation and maintenance;
7. a clear reporting structure and agreed reporting formats;
8. a clear and specified process of change management;
9. access control policy, covering:
    i. the different reasons, requirements, and benefits that make the access by the third-party necessary;
    ii. permitted access methods (e.g., multi-factor authentication), and the control and use of unique identifiers such as user IDs and passwords;
    iii. an authorization process for user access and privileges;
    iv. a requirement to maintain a list of individuals authorized to use the services being made available, and what their rights and privileges are with respect to such use;
    v. a statement that all access that is not explicitly authorized is forbidden; and
    vi. a process for revoking access rights or interrupting the connection between systems;
10. arrangements for reporting, notification (e.g., how, when and to whom), and investigation of information security incidents and security breaches, as well as violations of the requirements in the agreement, stating:
    i. the third-party, following the discovery of a breach of unsecured covered information, notifies the organization of such breach, including the identification of each individual whose unsecured PII has been, or is reasonably believed by the business partner to have been, accessed, acquired, or disclosed during such breach;
    ii. all notifications are made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach if the BA is an agent of the organization, otherwise the timing of the notification is explicitly addressed in the contract if the BA is not an agent of the organization;
    iii. evidence is maintained demonstrating that all notifications were made without unreasonable delay; and
    iv. any other information that may be needed in the notification to individuals, either at the time the notice of the breach is provided, or promptly thereafter as information becomes available.
11. a description of the product or service to be provided, and a description of the information to be made available along with its security classification (see CSF 07.d);
12. the target level of service and unacceptable levels of service;
13. the definition of verifiable performance criteria, their monitoring and reporting;
14. the right to monitor, and revoke, any activity related to the organization's assets;
15. the right to audit responsibilities defined in the agreement, to have those audits carried out by a third-party, and to enumerate the statutory rights of auditors;
16. the penalties exacted in the event of any failure in respect of the above;
17. the establishment of an escalation process for problem resolution;
18. service continuity requirements, including measures for availability and reliability, in accordance with an organization's business priorities;
19. the respective liabilities of the parties to the agreement;
20. responsibilities with respect to legal matters and how it is ensured that the legal requirements are met (e.g., data protection legislation) especially taking into account different national legal systems if the agreement involves co-operation with organizations in other countries (see 6.1);
21. intellectual property rights (IPRs) and copyright assignment (see 6. b) and protection of any collaborative work (see 5.e); and
22. conditions for renegotiation/termination of agreements:

	i. a contingency plan is in place in case either party wishes to terminate the relation before the end of the agreements; ii. renegotiation of agreements if the security requirements of the organization change; and iii. current documentation of asset lists, licenses, agreements, or rights relating to them. The organization establishes and documents personnel security requirements including security roles and responsibilities for third-party providers that are coordinated and aligned with internal security roles and responsibilities and monitor provider compliance. A screening process is also carried out for contractors and third-party users. Where contractors are provided through an organization, the contract with the organization clearly specifies the organization's responsibilities for screening and the notification procedures they need to follow if screening has not been completed or if the results give cause for doubt or concern. In the same way, the agreement with the third-party clearly specifies all responsibilities and notification procedures for screening. The organization requires third-party providers to notify a designated individual or role (e.g., a member of the contracting or supply chain function) of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within 15 calendar days.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 201 CMR 17.03(2)(f) 45 CFR Part § 164.314(a)(1) HIPAA.SR-0 45 CFR Part § 164.314(a)(2)(i)(A) HIPAA.SR-0 45 CFR Part § 164.314(a)(2)(i)(B) HIPAA.SR-0 45 CFR Part § 164.314(a)(2)(i)(C) HIPAA.SR-0 45 CFR Part § 164.314(a)(2)(ii) HIPAA.SR-0 45 CFR Part § 164.410(a)(1) HIPAA.BN-1 45 CFR Part § 164.410(c)(1) HIPAA.BN-0 45 CFR Part § 164.410(c)(2) HIPAA.BN-0 AICPA 2017 CC1.4 AICPA 2017 CC9.2 AICPA 2017 P6.1 AICPA 2017 P6.4 AICPA 2017 P6.5 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMMC v1.0 RM.4.148-1 CMSRs v3.1 PS-07 (HIGH; MOD) CRR v2016 EDM:G3.Q1 CRR v2016 EDM:G3.Q3 CRR v2016 EDM:G3.Q4 CRR v2016 EDM:MIL2.Q1 CSA CCM v3.0.1 STA-03 CSA CCM v3.0.1 STA-05 De-ID Framework v1 Third-party Assurance: General EU GDPR Article 32(4) FedRAMP PS-7 FFIEC IS v2016 A.3.3 FFIEC IS v2016 A.6.31(c) FFIEC IS v2016 A.6.31(e) FFIEC IS v2016 A.6.31(f) FFIEC IS v2016 A.6.31(g) IRS Pub 1075 v2016 9.3.13.7 ISO/IEC 27002:2013 15.1.1 ISO/IEC 27002:2013 15.1.2 ISO/IEC 27002:2013 15.1.3 ISO/IEC 27002:2013 7.1.1 ISO/IEC 27799:2016 15.1.1 ISO/IEC 27799:2016 15.1.2 ISO/IEC 27799:2016 15.1.3 ISO/IEC 27799:2016 7.1.1 MARS-E v2 PS-7 NIST Cybersecurity Framework v1.1 DE.CM-6 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 ID.GV-2

	NIST Cybersecurity Framework v1.1 PR.AT-3 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 PS-6a[HML]{2} NIST SP 800-53 R4 PS-7a[HML]{0} NIST SP 800-53 R4 PS-7c[HML]{0} NIST SP 800-53 R4 SA-10(4)[S]{2} NIST SP 800-53 R4 SA-10(5)[S]{2} NIST SP 800-53 R4 SA-10(6)[S]{3} NRS 603A.210.2 NRS 603A.215.1 NY DOH SSP v3.1 PS-7a[M]-0 NY DOH SSP v3.1 PS-7b[M]-0 NY DOH SSP v3.1 PS-7c[M]-0 NY DOH SSP v3.1 SA-9a[M]-2 PCI DSS v3.2.1 12.8.2 PCI DSS v3.2.1 12.8.5 PCI DSS v3.2.1 12.9 PCI DSS v3.2.1 2.6 PMI DSP Framework PR.DS-1 PMI DSP Framework RS-1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CRR V2016 Subject to FedRAMP Certification Subject to FTC Red Flags Rule Subject to IRS Pub 1075 Compliance
Level 2 Implementation:	Level 1 plus: Organizations employ formal contracts that, at a minimum, specify: 1. the confidential nature and value of the covered information; 2. the security measures to be implemented and/or complied with, including the organization's information security requirements as well as appropriate controls required by applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; 3. limitations to access to these services by third-parties; 4. the service levels to be achieved in the services provided; 5. the format and frequency of reporting to the organization's Information Security Management Forum; 6. the arrangement for representation of the third-party in appropriate organization meetings and working groups; 7. the arrangements for compliance auditing of the third-parties; 8. the penalties exacted in the event of any failure in respect of the above; and 9. the requirement to notify a specified person or office of any personnel transfers or terminations of third-party personnel working at organizational facilities with organizational credentials, badges, or information system privileges within one business day.

Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 16 CFR Part § 681.1 (e)(4) CMSRs v3.1 SA-09 (HIGH; MOD) CRR v2016 EDM:G1.Q1 EU GDPR Article 32(4) FedRAMP SA-9 FFIEC IS v2016 A.3.3 FFIEC IS v2016 A.6.31(c) FFIEC IS v2016 A.6.31(e) IRS Pub 1075 v2016 9.3.15.7 IRS Pub 1075 v2016 9.4.1 MARS-E v2 SA-9 NIST Cybersecurity Framework v1.1 DE.CM-6 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 ID.SC-1 NIST Cybersecurity Framework v1.1 PR.AT-3 NIST Cybersecurity Framework v1.1 PR.IP-11

Level Cloud Service Providers	**Implementation Requirements**
Level Cloud Service Providers Implementation:	Mutually-agreed upon provisions and/or terms are established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence. Supply chain agreements (e.g., SLAs) between providers and customers (tenants) incorporate at least the following mutually-agreed upon provisions and/or terms: 1. Scope of business relationship and services offered e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations; 2. Information security requirements, provider, and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to effectively enable governance, risk management, assurance, and legal, statutory, and regulatory compliance obligations by all impacted business relationships; 3. Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts; 4. Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain); 5. Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed; 6. Expiration of the business relationship and treatment of customer (tenant) data impacted; and 7. Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence. Service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream) are reviewed consistently, and no less than annually, to identify any non-conformance to established agreements. The reviews result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.

	Third-party service providers demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery-level agreements included in third-party contracts. Third-party reports, records, and services undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.

Level Community Supplemental Reqs 02	Implementation Requirements
Level Community Supplemental Reqs 02 Implementation:	The organization executes service contracts for incident management through an outside legal party to ensure client/attorney confidentiality.

Level FTI Custodians	Implementation Requirements
Level FTI Custodians Implementation:	Organizations ensure acquisition contracts contain appropriate language from IRS Pub 1075 v2014 Exhibit 7, Safeguarding Contract Language. Organizations must establish security policies and procedures based on IRS Publication 1075 for how FTI is stored, handled, and accessed inside the cloud through a legally binding contract or Service Level Agreement (SLA) with its third-party Cloud provider. Additional SLA requirements include but are not limited to: 1. FTI must be encrypted in transit within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant and operate using the FIPS 140-2 compliant module. 2. FTI may need to be encrypted while at rest in the Cloud, depending upon the security protocols inherent in the Cloud. If the cloud environment cannot appropriately isolate FTI, encryption is a potential compensating control. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant and operate using the FIPS 140-2 compliant module. 3. Storage devices where FTI has resided must be securely sanitized or destroyed using methods acceptable by NSA and Central Security Service (CSS). Organization-defined security controls for third-party arrangements (e.g., in cloud service providers) must be identified, documented (e.g., in a legally-binding contract or SLA), and implemented. The defined security controls, as implemented, must comply with the requirements specified in IRS Pub 1075 v2014.

Level GDPR	Implementation Requirements
Level GDPR Implementation:	Where two or more data controllers jointly determine the purposes and means of processing, they are joint controllers. They, in a transparent manner, determine their respective responsibilities for compliance with the obligations under GDPR, in particular as regards the exercising of the rights of the data subject and their respective duties to provide information regarding access to personal data, whether obtained by the controller from the subject or from another source, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by EU or Member State law to which the controllers are subject. This arrangement duly reflects the respective roles and relationships of the joint controllers vis-a-vis the data subjects, and the essence of the arrangement is made available to the data subject. The data controllers involved in the arrangement specifically allows a data subject to exercise the subjects rights under the GDPR in respect of and against each of the controllers. The processor does not engage another processor without prior specific or general written authorization of the controller. In the case of general written authorization, the

processor informs the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

Processing by a processor is governed by a written contract or other legal act (instrument) under Union or Member State law, including one in electronic form, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act (instrument) stipulates that the processor:

1. processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor informs the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
2. ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
3. takes all measures required pursuant by the EU GDPR for the security of processing personal data;
4. respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
5. taking into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
6. assists the controller in ensuring compliance with the obligations for the security of personal data, including the security of processing and data breach notification to the supervisory authority and data subject, data protection impact assessments and prior consultation with a supervisory authority, taking into account the nature of processing and the information available to the processor;
7. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
8. makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in the contract or other legal act (instrument) and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller, and immediately inform the controller if, in the processors opinion, an instruction infringes the EU GDPR or other EU or Member State data protection provision.

The processor requires the same data protection obligations in a written contract or other legal act (instrument) under EU or Member State law, including one in electronic form, where it engages another processor for carrying out specific processing activities on behalf of the controller, and in particular provides sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the EU GDPR.

The data controller ensures a processor and any person acting under the authority of the controller or of the processor, who has access to personal data, does not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

The controller and processor take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not

	process them except on instructions from the controller unless he or she is required to do so by Union or Member State law.

Level HIE Implementation Requirements	
Level HIE Implementation:	As part of the agreement with the connecting organizations, the HIE specifies the requirements of the connecting organization to define and communicate to the HIE access roles for the connecting organization's employees. The agreement specifies that it is the sole responsibility of the connecting organization to appropriately restrict access in accordance with federal and state requirements (e.g., mental health information). As part of the agreement with the connecting organizations, the HIE specifies the requirements of connecting organizations to request and receive detailed access logs (see 09.aa) related to the connecting organization's records.

Level HIX Implementation Requirements	
Level HIX Implementation:	The organization ensures that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance.

Level PCI Implementation Requirements	
Level PCI Implementation:	The organization identifies and documents information about which PCI DSS requirements are managed by each service provider, and which are managed by the organization.

Level Supplemental Requirements	Implementation Requirements
Level Supplemental Requirements Implementation:	Supplier complies to requirements under the supplier agreement, including maintaining and adhering to documented processes for (i) reviewing and scanning software developed or customized for the organization to find and remediate malicious code and/or security vulnerabilities prior to initial deployment, and making scan results and remediation plans available to the organization upon request; (ii) cooperating with the organization and taking all reasonable and necessary steps to isolate, mitigate, terminate, and/or remediate all known or suspected threats within 90 days of notification of a threat to the organization or its customers' nonpublic information resources originating from the supplier's network; and (iii) notifying and cooperating with the organization upon discovery of a supplier's noncompliance with the organization's security requirements, or of a known or suspected threat/vulnerability impacting the organization or its customers, and to take all reasonable and necessary steps to isolate, mitigate, and/or remediate such noncompliance or threat/vulnerability within 90 days. Supplier maintains and adheres to any business continuity plan and/or disaster recovery plan requirements under the agreement.

Control Category: 06.0 - Compliance

Objective Name: 06.01 Compliance with Legal Requirements

Control Objective:	To ensure that the design, operation, use, and management of information systems adheres to applicable laws, statutory, regulatory, or contractual obligations, and any security requirements.

Control Reference: 06.a Identification of Applicable Legislation

Control Specification:	All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.
Factor Type:	Organizational
Topics:	Awareness and Training; Documentation and Records; Policies and Procedures; Requirements (Legal and Contractual)

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to FTC Red Flags Rule Subject to HIPAA Security Rule Subject to NY OHIP Moderate-Plus Security Baseline Subject to State of Massachusetts Data Protection Act
Level 1 Implementation:	All relevant statutory, regulatory, and contractual requirements are explicitly defined and formally documented for each information system type. The specific controls and individual responsibilities to meet these requirements are similarly defined and documented. These controls are communicated to the user community through the documented security training and awareness programs.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(3) 1 TAC § 390.2(a)(4)(B)(xviii)(I) 16 CFR Part § 681 Appendix A VII(a) 16 CFR Part § 681 Appendix A VII(b) 16 CFR Part § 681 Appendix A VII(c) 16 CFR Part § 681 Appendix A VII(d) 201 CMR 17.03(1) 45 CFR Part § 164.316(a) HIPAA.SR-2 CSA CCM v3.0.1 AAC-03 FFIEC IS v2016 A.4.5 ISO/IEC 27002:2013 18.1.1 ISO/IEC 27002:2013 7.2.2 ISO/IEC 27799:2016 18.1.1 ISO/IEC 27799:2016 7.2.2 MARS-E v2 PM-15 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 PR.AT-3 NY DOH SSP v3.1 AT-1a[M]-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to NY OHIP Moderate-Plus Security Baseline
Level 2 Implementation:	Level 1 plus: Join industry trade associations, subscribe to thought leadership and market research organizations, or establish some other reliable process to stay abreast of business sector, industry, technology, infrastructure, legal and regulatory environment trends that may impact your organization security policies. Incorporate the consequences of these trends into the development or update of the IT policies and procedures.
Level 2 Control Standard Mapping:	AICPA 2017 CC1.3 CMSRs v3.1 PM-15 (HIGH; MOD) CSA CCM v3.0.1 AAC-03 FFIEC IS v2016 A.4.5 ISO/IEC 27002:2013 18.1.1 ISO/IEC 27002:2013 6.1.4 ISO/IEC 27799:2016 18.1.1 ISO/IEC 27799:2016 6.1.4 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 PR.IP-7 NIST Cybersecurity Framework v1.1 RS.CO-5 NY DOH SSP v3.1 PM-15a[M]-1 NY DOH SSP v3.1 PM-16[M]-3

Control Reference: 06.b Intellectual Property Rights

Control Specification:	Detailed procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights, and on the use of proprietary software products.
Factor Type:	Organizational
Topics:	Documentation and Records; Policies and Procedures; Requirements (Legal and Contractual)

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate)

	Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline
Level 1 Implementation:	Procedures are developed and implemented to ensure compliance with any legislative, regulatory, or contractual requirements that may place restrictions on the copying of proprietary material including copyrights, design rights, or trademarks. Specifically, the following controls are in place: 1. acquiring software only through known and reputable sources, to ensure that copyright is not violated; 2. maintaining proof and evidence of ownership of licenses, master disks, manuals, etc.; 3. implementing controls to ensure that any maximum number of users permitted is not exceeded; 4. carrying out annual checks that only authorized software and licensed products are installed; 5. developing and providing a policy for maintaining agreed upon license conditions; 6. using manual audit tools; 7. complying with terms and conditions for software and information obtained from public networks; and 8. use of proprietary software must also be in compliance with encryption, export and local data privacy regulations.
Level 1 Control Standard Mapping:	ISO/IEC 27002:2013 18.1.2 ISO/IEC 27799:2016 18.1.2 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST SP 800-53 R4 CM-10b[HML]{0} NIST SP 800-53 R4 SI-14(1)[S]{2} NY DOH SSP v3.1 CM-7(2)a[M]-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate)
Level 2 Implementation:	Level 1 plus: The following controls are in place: 1. publishing an intellectual property rights compliance policy which defines the legal use of software and information products; 2. maintaining awareness of policies to protect intellectual property rights, and giving notice of the intent to take disciplinary action against personnel breaching them;

	3. maintaining appropriate asset registers, and identifying all assets with requirements to protect intellectual property rights; 4. developing and providing a policy for disposing software or transferring software to others; 5. not duplicating, converting to another format, or extracting from commercial recordings (film, audio) other than permitted by copyright law; and 6. not copying, in full or in part, books, articles, reports or other documents, other than permitted by copyright law.
Level 2 Control Standard Mapping:	ISO/IEC 27002:2013 18.1.2 ISO/IEC 27799:2016 18.1.2 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST SP 800-53 R4 SI-12[HML]{4}

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: The organization controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 CM-10 (HIGH; MOD) FedRAMP CM-10 IRS Pub 1075 v2016 9.3.5.10 MARS-E v2 CM-10 NIST Cybersecurity Framework v1.1 DE.CM-3 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 PR.IP-1 NIST SP 800-53 R4 CM-10c[HML]{0} NY DOH SSP v3.1 CM-10b[M]-0 NY DOH SSP v3.1 CM-10c[M]-0

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The organization must establish restrictions on the use of open-source software, and any open-source software used by the organization must: 1. be legally licensed; 2. be authorized; and 3. adhere to the organizations secure configuration policy.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	The organization must establish restrictions on the use of open-source software, and any open-source software used by the organization must: 1. Be legally licensed; 2. Be approved by the agency IT department; and 3. Adhere to a secure configuration baseline checklist from the U.S. Government or industry.

Control Reference: 06.c Protection of Organizational Records

Control Specification:	Important records shall be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Cryptography; Data Loss Prevention; Documentation and Records; Policies and Procedures; Requirements (Legal and Contractual)

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 3 Subject to HIPAA Security Rule Subject to Joint Commission Accreditation Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to State of Massachusetts Data Protection Act Subject to the State of Nevada Security of Personal Information Requirements
Level 1 Implementation:	Important records, such as contracts, personnel records, financial information, client/customer information, etc., of the organization are protected from loss, destruction, and falsification. Security controls, such as access controls, encryption, backups, electronic signatures, locked facilities, or containers, etc., are implemented to protect these essential records and information. Guidelines are issued by the organization on the ownership, classification, retention, storage, handling and disposal of all records and information. Designated senior management within the organization review and approve the security categorizations and associated guidelines.

	All regulatory and legislative retention requirements are met. The organization's formal policies and procedures, other critical records (e.g., results from a risk assessment) and disclosures of individuals' protected health information made is retained for a minimum of six years. For electronic health records, the organization must retain records of disclosures to carry out treatment, payment, and health care operations for a minimum of three years. The organization documents compliance with the notice requirements by retaining copies of the notices issued by the covered entity for a period of six years and, if applicable, any written acknowledgements of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgement. The organization documents restrictions in writing and formally maintain such writing, or an electronic copy of such writing, as an organizational record for a period of six years. The organization documents and maintains records (PII) that are subject to access by individuals and the titles of the persons or office responsible for receiving and processing requests for access by individuals as organizational records for a period of six years.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(3) 1 TAC § 390.2(a)(4)(A)(xi) 201 CMR 17.03(2)(g) 21 CFR Part 11.10(c) 21 CFR Part 11.30 45 CFR Part § 164.316(b)(1)(ii) HIPAA.SR-2 45 CFR Part § 164.520(e) HIPAA.PR 45 CFR Part § 164.522(a)(3) HIPAA.PR 45 CFR Part § 164.524(e) HIPAA.PR 45 CFR Part § 164.530(j) HIPAA.PR 45 CFR Part § 164.530(j)(2) HIPAA.PR AICPA 2017 C1.1 AICPA 2017 C1.2 AICPA 2017 P4.2 CMMC v1.0 AM.3.036-0 CMSRs v3.1 RA-02 (HIGH; MOD) CRR v2016 CM:G2.Q3 FedRAMP RA-2 FFIEC IS v2016 A.6.18(a) FFIEC IS v2016 A.6.18(b) IRS Pub 1075 v2016 4.2 IRS Pub 1075 v2016 9.3.6.7 ISO/IEC 27002:2013 18.1.3 ISO/IEC 27002:2013 8.2.1 ISO/IEC 27799:2016 18.1.3 ISO/IEC 27799:2016 8.2.1 MARS-E v2 RA-2 NIST Cybersecurity Framework v1.1 ID.AM-5 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 PR.PT-1 NIST SP 800-53 R4 AC-16(2)[S]{2} NIST SP 800-53 R4 CP-9(7)[S]{0} NIST SP 800-53 R4 CP-9[HML]{4} NIST SP 800-53 R4 RA-2c[HML]{0} NRS 603A.210.1 NRS 603A.210.3 NY DOH SSP v3.1 MP-6.PII1[M]-3 NY DOH SSP v3.1 MP-6a[M]-2 NY DOH SSP v3.1 RA-2.PII[M]-0 NY DOH SSP v3.1 RA-2c[M]-0 TJC IM.02.01.03, EP 6

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions

	Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CRR V2016 Subject to EHNAC Accreditation Subject to FedRAMP Certification Subject to FISMA Compliance Subject to HIPAA Security Rule Subject to HITRUST De-ID Framework Requirements Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Privacy) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The organization establishes a formal record retention program that addresses: 1. the secure disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of covered and/or confidential information (see 09.p and 08.l); 2. coverage over all storage of covered and/or confidential information; and 3. a programmatic review process (automatic or manual) to identify and remove covered and/or confidential information that exceeds the requirements of the data retention policy on a quarterly basis. Detailed procedures for record storage, access, retention, and destruction are implemented. In doing so, the following controls are implemented: 1. a retention schedule is drawn up identifying essential record types and the period of time for which they must be retained; 2. an inventory of sources of key information is maintained; 3. any related cryptographic keys are kept securely and made available only when necessary; and 4. any related cryptographic keying material and programs associated with encrypted archives or digital signatures are also stored to enable decryption of the records for the length of time the records are retained.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(c) 21 CFR Part 11.30 45 CFR Part § 164.316(b)(1)(ii) HIPAA.SR-3 45 CFR Part § 164.316(b)(1)(ii) HIPAA.SR-4 45 CFR Part § 164.530(j)(2) HIPAA.PR AICPA 2017 C1.1 AICPA 2017 C1.2 CMSRs v3.1 AU-11 (HIGH; MOD) CMSRs v3.1 DM-02 (HIGH; MOD)

	CMSRs v3.1 DM-02(01) (HIGH; MOD) CMSRs v3.1 SI-12 (HIGH; MOD) CRR v2016 CM:G2.Q3 De-ID Framework v1 Retention: Data Retention Policy FedRAMP SI-12 FFIEC IS v2016 A.6.18(a) FFIEC IS v2016 A.6.18(b) IRS Pub 1075 v2016 9.3.17.9 IRS Pub 1075 v2016 9.3.3.11 ISO/IEC 27002:2013 18.1.3 ISO/IEC 27799:2016 18.1.3 MARS-E v2 AU-11 MARS-E v2 DM-2 MARS-E v2 DM-2(1) MARS-E v2 SI-12 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 PS.DS-3 NIST SP 800-53 R4 AU-11(1)[S]{1} NIST SP 800-53 R4 DM-2c[P]{0} NIST SP 800-53 R4 SI-12[HML]{1} NRS 603A.215.1 NY DOH SSP v3.1 AC-6(7).NYS4[MN]-0 PCI DSS v3.2.1 3.1 PMI DSP Framework PR.DS-2

Level CMS Implementation Requirements

Level CMS Implementation:	The organization retains output including, but not limited to audit records, system records, business and financial reports, and business records, from the information system in accordance with CMS Policy and all applicable National Archives and Records Administration (NARA) requirements.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	The organization employs a permanent system of standardized records of request for disclosure of FTI and maintains the records for five years, or the applicable records control schedule, whichever is longer. To support the audit of FTI activities, all organizations must ensure that audit information is archived for seven years to enable the recreation of computer-related accesses to both the operating system and to the application wherever FTI is stored, support after-the-fact investigations of security incidents and meet regulatory and agency information retention requirements.

Level HIPAA Implementation Requirements

Level HIPAA Implementation:	If retained, the organization ensures individually identifiable information is safeguarded for a period of 50 years following the date of death of the individual. The covered entity documents and maintains accountings of disclosure as organizational records for a period of six years, including the information required for disclosure, the written accounting provided to the individual, and the titles of the persons or offices responsible for receiving and processing requests for an accounting. The organization's formal policies and procedures, other critical records (e.g., results from a risk assessment) and disclosures of individuals' protected health information made is retained for a minimum of six years. For electronic health records, the organization must retain records of disclosures to carry out treatment, payment and health care operations for a minimum of three years.

Level HIX Implementation Requirements	
Level HIX Implementation:	The organization retains output including, but not limited to audit records, system records, business and financial reports, and business records, from the information system for 10 years or in accordance Administering Entity organizational requirements.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation:	The information system implements cryptographic mechanisms, in transit and at rest, as defined in the HHS Standard for Encryption of Computing Devices and Information, and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. The information system protects the confidentiality and integrity of information at rest, as defined in the HHS Standard for Encryption of Computing Devices and Information. Systems processing, storing, or transmitting PHI: HIPAA requires that the following actions, activities, and assessments relating to the security of systems containing PHI be documented and retained for at least six [6] years from the date of its creation or the date when it was last in effect, whichever is later: (i) decisions regarding addressable implementation specifications, specifically why it would not be reasonable and appropriate to implement the implementation specification in question; (ii) a user's right of access to a workstation, transaction, program, or process; (iii) security incidents and their outcomes; (iv) satisfactory assurances that a business associate will appropriately safeguard PHI, this documentation is recorded in a written contract or other arrangement with the business associate and must meet the applicable requirements of business associate agreements - if satisfactory assurances cannot be attained, document the attempt and the reasons that these assurances cannot be obtained; (v) repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks); and (vi) changes to organizational policies and procedures.

Level PCI Implementation Requirements	
Level PCI Implementation:	The organization keeps cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: 1. Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements; 2. Processes for secure deletion of data when no longer needed; 3. Specific retention requirements for cardholder data; and 4. A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.

Level Supplemental Requirements Implementation Requirements	
Level Supplemental Requirements Implementation:	Guidelines are issued by the organization on the ownership, classification, retention, storage, handling, return, and disposal of all records and information. The organization maintains controls to detect and terminate unauthorized attempts to access, modify, store, and/or handle in-scope information. The confidentiality and integrity of information is protected at rest and in transit in the following scenarios using a cryptographic algorithm with minimum key lengths of 256 bits for symmetric and 2048 bits for asymmetric, and proper key management practices

	including keys with a maximum lifetime of two years for: (i) all in-scope information (ISI) transmitted over untrusted networks; (ii) all ISI stored or transmitted using mobile and portable devices; (iii) all wireless networking technologies used to transmit ISI; (iv) all ISI stored within, or transmitted to, from, and within non-organizational cloud services; and (v) all sensitive personal information (SPI)/sensitive customer data (SCD) stored or transmitted over all networks, including trusted networks. Separation between operational information and non-production (development, test/quality assurance) environments is maintained.

Control Reference: 06.d Data Protection and Privacy of Covered Information

Control Specification:	Data protection and privacy shall be ensured as required in relevant legislation, regulations, and contractual clauses. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Awareness and Training; Data Loss Prevention; IT Organization and Management Roles and Responsibilities; Monitoring; Requirements (Legal and Contractual); Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 3 Subject to Community Supplemental Requirements 002 Subject to HIPAA Security Rule Subject to Joint Commission Accreditation Subject to NIST 800-171 Derived Level Subject to NY OHIP Moderate-Plus Security Baseline Subject to Texas Health and Safety Code Subject to the State of Nevada Security of Personal Information Requirements
Level 1 Implementation:	An organizational data protection and privacy policy is developed and implemented. This policy is communicated to all persons involved in the processing of covered and/or confidential information. Compliance with this policy and all relevant data protection legislation and regulations is supported by management structure and control. Responsibility for handling covered and/or confidential information and ensuring awareness of the data protection principles is dealt with in accordance with relevant legislation and regulations. Technical security controls - including access controls, special authentication requirements, and monitoring - and organizational measures to protect covered and/or confidential information are implemented. There is an appointment of a person responsible, such as a data protection officer or privacy officer, who is responsible for the organizations individual privacy protection program, and the officer reports directly to the highest management level of the organization (e.g., a CEO). The data protection officer is designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill required tasks.

Responsibilities include the development and implementation of privacy policies and procedures, serving as the point of contact for all privacy-related issues, including the receipt of privacy-related complaints, and providing privacy-related guidance to managers, users, and service providers on their individual responsibilities and the specific procedures that are followed. The data protection officer will, in the performance of those tasks, have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

The data protection officer may fulfil other tasks and duties; however, the organization ensures that any such tasks and duties do not result in a conflict of interests.

Where required by legislation, consent is obtained before any PII (e.g., about a client/customer) is emailed, faxed, or communicated by telephone conversation, or otherwise disclosed, to parties external to the organization.

The information system protects the confidentiality and integrity of information at rest. Covered and/or confidential information, at minimum, is rendered unusable, unreadable, or indecipherable anywhere it is stored, including on personal computers (laptops, desktops) portable digital media, backup media, servers, databases, or in logs, by using any of the following approaches:

1. full disk encryption (mandatory for laptops and other mobile devices that support full disk encryption, see 01.x);
2. virtual disk encryption;
3. volume disk encryption; and
4. file and folder encryption.

The encryption approach is implemented using one or a combination of the following:

1. one-way hashes based on strong cryptography;
2. truncation; and
3. strong cryptography with associated key-management processes and procedures.

The system implements one of the following encryption algorithms:

1. AES-CBC (AES in Cipher Block Chaining mode) with a symmetric 128-bit key minimum (256-bit key for cloud services) or asymmetric 2048-bit key minimum (3072-bit key for cloud services);
2. Triple DES (3DES-CBC);

If encryption is not applied because it is determined to not be reasonable or appropriate, the organization documents its rationale for its decision or uses alternative compensating controls other than encryption if the method is approved and reviewed annually by the CISO.

If disk encryption is used (rather than file- or column-level database encryption), logical access is managed independently of native operating system access control mechanisms, and decryption keys are not tied to user accounts. See NIST SP 800-111 Guide to Storage Encryption Technologies for End User Devices for more information on implementing strong cryptography technologies.

Organizations explicitly identify and ensure the implementation of security and privacy protections for the transfer of organizational records, or extracts of such records, containing sensitive personal information to a state or federal agency or other regulatory body that lawfully collects such information.

The organization specifies where covered and/or confidential information can be stored.

Covered and/or confidential information storage is kept to a minimum.

	The controller and the processor designate a data protection officer in any case where: 1. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; 2. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope, and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or 3. the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences. The organization supports the data protection officer in performing the tasks required by law or regulation by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain the data protection officers expert knowledge. The organization ensures that the data protection or privacy officer does not receive any instructions regarding the exercise of those tasks, and the officer is bound by secrecy or confidentiality concerning the performance of the of those tasks, in accordance with applicable law or regulation. The officer is not dismissed or penalized by the organization for performing those tasks.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(4) 1 TAC § 390.2(a)(4)(A)(i) 1 TAC § 390.2(a)(4)(A)(xi) 1 TAC § 390.2(a)(4)(A)(xv) 21 CFR Part 11.30 23 NYCRR 500.15(a)(1) 45 CFR Part § 164.312(a)(2)(iv) HIPAA.SR-2 45 CFR Part § 164.312(e)(2)(ii) HIPAA.SR-0 45 CFR Part § 164.530(a) HIPAA.PR 45 CFR Part § 164.530(a)(2)(i) HIPAA.PR 45 CFR Part § 164.530(b) HIPAA.PR 45 CFR Part § 164.530(c)(1) HIPAA.PR AICPA 2017 CC6.1 CIS CSC v7.1 14.8 CMMC v1.0 SC.3.191-0 CMSRs v3.1 AR-01 (HIGH; MOD) CMSRs v3.1 AR-02 (HIGH; MOD) CMSRs v3.1 SC-12(01) (HIGH) CMSRs v3.1 SC-28 (HIGH; MOD) CRR v2016 CM:G2.Q3 CSA CCM v3.0.1 EKM-01 CSA CCM v3.0.1 EKM-02 CSA CCM v3.0.1 EKM-03 CSR002 v2018 11.2-6-0 De-ID Framework v1 Data Storage: General De-ID Framework v1 Storage (Minimal Locations Authorized): Policy EU GDPR Article 37(1) EU GDPR Article 37(2) EU GDPR Article 37(5) EU GDPR Article 38(1) EU GDPR Article 38(2) EU GDPR Article 38(3) EU GDPR Article 39(1) EU GDPR Article 39(2) FedRAMP SC-28 FedRAMP SC-28(1) FFIEC IS v2016 A.6.18(a) FFIEC IS v2016 A.6.30 HITRUST IRS Pub 1075 v2016 4.2 IRS Pub 1075 v2016 8.3 IRS Pub 1075 v2016 9.3.16.15 IRS Pub 1075 v2016 9.3.6.7 ISO/IEC 27002:2013 18.1.4 ISO/IEC 27799:2016 18.1.4 ISO/IEC 27799:2016 7.12.2.2 MARS-E v2 AR-1

	MARS-E v2 AR-2 MARS-E v2 SC-12 MARS-E v2 SC-28 NIST 800-171 r2 3.13.16-0 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.DS-2 NRS 603A.210.1 NRS 603A.215.1 NY DOH SSP v3.1 CP-9.IS2[M]-3 OCR Guidance for Unsecured PHI (1)(i) OCR Guidance for Unsecured PHI (1)(ii) PCI DSS v3.2.1 3.4 PMI DSP Framework PR.DS-1 PMI DSP Framework PR.DS-2 TJC IM.02.01.03, EP 2

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to FedRAMP Certification Subject to FISMA Compliance Subject to HITRUST De-ID Framework Requirements Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: Covered information storage is kept to a minimum. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy. The organization implements technical means to ensure covered information is stored in organization-specified locations.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 SI-12 (HIGH) De-ID Framework v1 Storage (Minimal Locations Authorized): Implementation FedRAMP SI-12 IRS Pub 1075 v2016 9.3.17.9 IRS Pub 1075 v2016 Exhibit 10 ISO/IEC 27002:2013 18.1.3 ISO/IEC 27799:2016 18.1.3 MARS-E v2 SI-12 NIST Cybersecurity Framework v1.1 ID.GV-3 NRS 603A.215.1 PCI DSS v3.2.1 3.1

Level CIS Implementation Requirements

Level CIS Implementation:	Access to encrypted information at rest requires a secondary authentication mechanism not integrated into the operating system.

Level De-ID Data Environment	Implementation Requirements
Level De-ID Data Environment Implementation:	Covered information is encrypted in transit whether internal or external to the organization's network, and, if not encrypted in transit, the organization must document its rationale.

Level FTI Custodians	Implementation Requirements
Level FTI Custodians Implementation:	Organizations are not allowed to make further disclosures of FTI to their agents or to a contractor unless authorized by statute. Organizations ensure that FTI will not be subject to public disclosure. FTI stored on deployed user workstations, in non-volatile storage, is encrypted with FIPS-validated or National Security Agency (NSA)-approved encryption during storage (regardless of location) except when no approved encryption technology solution is available that addresses the specific technology.

Level GDPR	Implementation Requirements
Level GDPR Implementation:	A data controller or processor, which is not established in the EU, designates in writing a representative in the EU, in one of the EU Member States where the data subjects are and whose personal data are processed in relation to the offering of goods or services to them, or whose behavior is monitored, UNLESS: 1. processing is occasional and: i. does not include special categories of personal data; ii. does not include personal data relating to criminal convictions and offenses; iii. is unlikely to result in a risk to the rights and liberties (freedoms) of natural persons, taking into account the nature, context, scope and purposes of the processing; or iv. the controller or processor is a public authority or body. The data controller or processor not established in the EU and which is required to designate an EU representative, mandates the representative to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with the EU GDPR, and such designation is without prejudice to legal actions that could be initiated against the controller or the processor themselves. A data protection officer is designated for a (i) controller, (ii) processor, (iii) group of undertakings, provided the officer is accessible from each establishment, or (iv) group of multiple public authorities or bodies, taking account of their organizational structure and size, in any case where: 1. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; 2. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

	3. the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences. The controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law, also designates a data protection officer, who may act for such associations and other bodies representing controllers or processors. The controller or the processor publishes the contact details of the data protection officer and communicate them to the supervisory authority. The data protection officer has at least the following tasks: 1. To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the EU GDPR and to other Union or Member State data protection provisions; 2. To monitor compliance with the EU GDPR, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; 3. To provide advice where requested as regards the data protection impact assessment and monitor its performance; 4. To cooperate with the supervisory authority; 5. To act as the contact point for the supervisory authority on issues relating to processing, including prior consultation with a supervisory authority, and to consult, where appropriate, with regard to any other matter.

Level Group Health Plans Implementation Requirements

Level Group Health Plans Implementation:	Group Health Plan plan documents incorporate provisions to require the plan sponsor to: i) implement administrative, physical, and technical safeguards to reasonably and appropriately protect electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan; ii) ensure that adequate separate is supported by reasonable and appropriate security measures; iii) ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and iv) report to the group health plan any security incident of which it becomes aware.

Level HIPAA Implementation Requirements

Level HIPAA Implementation:	Workstations that can access covered and/or confidential information are configured with specifications that address: 1. proper functions to be performed, 2. the manner in which those functions are to be performed, and 3. physical attributes of the surroundings.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	Access to PII from external information systems (including, but not limited to, personally owned information systems/devices) is limited to those organizations and individuals with a binding agreement to terms and conditions of privacy requirements which protect the PII.

	At a minimum, controls must include implementation of either full-device or virtual container encryption to reduce the vulnerability of PII contained on mobile devices. Systems processing, storing, or transmitting PII (to include PHI): The information system protects the confidentiality and integrity of personally identifiable information (PII). The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of CMS sensitive information as defined in the Risk Management Handbook (RMH), Volume 1, Chapter 10, CMS Risk Management Terms, Definitions, and Acronyms. Systems processing, storing, or transmitting PII (to include PHI): The organization must (i) encrypt data at rest in mobile devices for confidentiality to protect against loss, theft, or compromise; (ii) encrypt data stored in network share drives to insure confidentiality; (iii) encrypt storage/back-up data where physical protection is either not available, not implemented, or not audited; (iv) if assurance is not provided by other means, encrypt personally identifiable information (PII) in a database; and (v) encrypt data stored in the cloud—whether the cloud is government or private. Encryption is required for data at rest for (i) desktops that access or contain State Entity (SE) PPSI; (ii) data stores (including but not limited to databases, file shares) that contain SE PPSI; (iii) all mobile devices, whether State issued or third party, that access or contain any SE information; and (iv) all portable storage devices containing any SE information. Encryption is required for data at rest when electronic PPSI is transported or stored outside of a State facility. The organization must follow specific precautions and Implementation Standards when performing fax transmission of PII or PHI: Transmit PII or PHI only to an authorized recipient.

Level PCI Implementation Requirements

Level PCI Implementation:	The organization renders the PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: 1. One-way hashes based on strong cryptography (hash must be of the entire PAN); 2. Truncation (hashing cannot be used to replace the truncated segment of the PAN); 3. Index tokens and pads (pads must be securely stored); and 4. Strong cryptography with associated key management processes and procedures. If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

Control Reference: 06.e Prevention of Misuse of Information Assets

Control Specification:	Users shall be deterred from using information assets for unauthorized purposes. *Required for HITRUST Certification CSF v9.6

Factor Type:	Organizational
Topics:	Authorization; Awareness and Training; Documentation and Records; IT Organization and Management Roles and Responsibilities; Media and Assets; Personnel; Third-parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 2 Subject to HIPAA Security Rule Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance
Level 1 Implementation:	The following procedures are implemented to ensure proper authorization and use of computer information assets: 1. notification to all employees that their actions may be monitored and that they consent to such monitoring (Note: the legality of such monitoring must be verified in each legal jurisdiction); 2. acceptable use agreements that are signed by all employees of an organization, contractors, and third-party users indicating that they have read, understand, and agree to abide by the rules of behavior before management authorizes access to the information system and its resident information. These acceptable use agreements are retained by the organization; 3. reviews and updates the rules of behavior every 365 days; and 4. requires individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules of behavior are revised/updated. Management approves the use of information assets. If any unauthorized activity is identified by monitoring or other means, this activity is brought to the attention of the individual manager concerned for consideration of appropriate disciplinary and/or legal action. All employees are informed in writing (e.g., when they sign rules of behavior or an acceptable use agreement) that violations of security policies may result in sanctions or disciplinary action (see 02.f).
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.308(a)(3)(ii)(A) HIPAA.SR-2 AICPA 2017 CC1.1 AICPA 2017 CC1.5 CMMC v1.0 AC.2.005-2 CMSRs v3.1 PL-04 (HIGH) CMSRs v3.1 PL-04 (HIGH; MOD) CMSRs v3.1 PS-08 (HIGH; MOD) FedRAMP PL-4 FedRAMP PS-8 IRS Pub 1075 v2016 9.3.12.3 IRS Pub 1075 v2016 9.3.13.8 MARS-E v2 PL-4 MARS-E v2 PS-8 NIST 800-171 r2 3.1.9-2 NIST Cybersecurity Framework v1.1 DE.CM-1

	NIST Cybersecurity Framework v1.1 DE.CM-3 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 PL-4b[HML]{2} NRS 603A.215.1 NY DOH SSP v3.1 AC-3(9).NYS[MN]-2 NY DOH SSP v3.1 PL-4b[M]-0 NY DOH SSP v3.1 PL-4c[M]-0 NY DOH SSP v3.1 PL-4e[M]-1 NY DOH SSP v3.1 PL-4e[M]-2 NY DOH SSP v3.1 PL-4f[M]-2 PCI DSS v3.2.1 12.3.1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 2 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to Supplemental Requirements Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: Computer login banners are displayed stating: 1. the computer being accessed is private; 2. unauthorized access is prohibited; 3. conditions for access (including consent to monitoring and recording), acceptable use, and access limitations; and 4. privacy and security notices. The user is required to acknowledge the login banner to continue with the log-on.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMMC v1.0 AC.2.005-1 CMSRs v3.1 AC-08 (HIGH; MOD) FedRAMP AC-8 IRS Pub 1075 v2016 9.3.1.8 MARS-E v2 AC-8 NIST 800-171 r2 3.1.9-1 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 AC-8[HML]{0} SR v6.4 24-0

Level CMS Implementation Requirements	
Level CMS Implementation:	The approved banner for CMS information systems reads: 1. you are accessing a U.S. Government information system, which includes: i. this computer, ii. this computer network, iii. all computers connected to this network, and iv. all devices and storage media attached to this network or to a computer on this network; and 2. this information system is provided for U.S. Government-authorized use only; 3. unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties; 4. by using this information system, you understand and consent to the following: i. you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system and, at any time, and for any lawful Government purpose, the Government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system. ii. any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose. For publicly accessible systems, the information system: 1. displays the system use information when appropriate, before granting further access; 2. displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. includes in the notice given to public users of the information system, a description of the authorized uses of the system.

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation:	The service provider determines elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the Joint Authorization Board (JAB). The service provider determines how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the Joint Authorization Board (JAB).

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation:	The IRS-approved warning banner must be applied at the application, database, operating system, and network device levels for all systems that receive, process, store, or transmit FTI. For publicly accessible systems, the information system must: 1. Display the IRS-approved warning banner granting further access; 2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Include a description of the authorized uses of the system.

	The warning banner must contain reference to the civil and criminal penalty sections of Title 26 Sections 7213, 7213A and 7431.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The information system (i) displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; the approved banner states: a) this warning banner provides privacy and security notices consistent with applicable federal laws, directives, and other federal guidance for accessing this Government system, which includes 1) this computer network, 2) all computers connected to this network, and 3) all devices and storage media attached to this network or to a computer on this network; b) this system is provided for Government authorized use only; c) unauthorized or improper use of this system is prohibited and may result in disciplinary action and/or civil and criminal penalties; d) personal use of social media and networking sites on this system is limited as to not interfere with official work duties and is subject to monitoring; e) by using this system, you understand and consent to the following: 1) “The Government may monitor, record, and audit your system usage, including usage of personal devices and email systems for official duties or to conduct HHS business. Therefore, you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this system. At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this system.” 2) “Any communication or data transiting or stored on this system may be disclosed or used for any lawful Government purpose;” (ii) retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and (iii) for publicly accessible systems: a) displays system use information when appropriate, before granting further access; b) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and c) includes a description of the authorized uses of the system. Systems processing, storing, or transmitting PII (to include PHI): Pursuant to OMB M-17-12, organizational rules of behavior must include a policy outlining the rules of behavior to safeguard personally identifiable information (PII) and identifying consequences and corrective actions for failure to follow these rules; consequences should be commensurate with level of responsibility and type of PII involved.

Control Reference: 06.f Regulation of Cryptographic Controls

Control Specification:	Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
Factor Type:	Organizational
Topics:	Cryptography; IT Organization and Management Roles and Responsibilities; Requirements (Legal and Contractual)

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1	

Regulatory Factors:	
Level 1 Implementation:	Legal advice is sought in relation to all relevant regulations by the organization. Compliance with all relevant regulations is reviewed on an annual basis at a minimum.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) ISO/IEC 27002:2013 18.1.1 ISO/IEC 27002:2013 18.1.2 ISO/IEC 27002:2013 18.1.3 ISO/IEC 27002:2013 18.1.4 ISO/IEC 27002:2013 18.1.5 ISO/IEC 27799:2016 18.1.1 ISO/IEC 27799:2016 18.1.2 NIST Cybersecurity Framework v1.1 ID.GV-3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The organization accounts for any country-specific regulations governing the use of cryptographic controls which may include the following: 1. import and/or export of computer hardware and software for performing cryptographic functions; 2. import and/or export of computer hardware and software which is designed to have cryptographic functions added to it; 3. restrictions on the usage of encryption; 4. mandatory or discretionary methods of access by the countries to information encrypted by hardware or software to provide confidentiality of content; and 5. mechanisms for authentication to a cryptographic module that meets U.S. requirements for such authentication (e.g., validation under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2), if applicable. Legal advice is specific to either the country where the cryptographic controls are used, or the country to which such controls are imported or exported.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 IA-07 (HIGH; MOD) CMSRs v3.1 SC-13 (HIGH; MOD) FedRAMP IA-7 FedRAMP SC-13

	IRS Pub 1075 v2016 9.3.16.9 IRS Pub 1075 v2016 9.3.7.7 ISO/IEC 27002:2013 18.1.5 ISO/IEC 27799:2016 18.1.5 MARS-E v2 IA-13(1) MARS-E v2 IA-7 MARS-E v2 ISC-13 NIST Cybersecurity Framework v1.1 ID.GV-3

Level CMMC Implementation Requirements

Level CMMC Implementation:	The organization employs cryptographic modules that are certified and that adhere to the minimum applicable standards when used to protect the confidentiality of information.

Level CMS Implementation Requirements

Level CMS Implementation:	When cryptographic mechanisms are used, the organization employs, at a minimum, FIPS 140-2 compliant and NIST-validated cryptography to protect unclassified information.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The organization uses a defined encryption methodology to encrypt personally identifiable information (PII) confidentiality impact level in backups at the storage location. The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

Objective Name: 06.02 Compliance with Security Policies and Standards, and Technical Compliance

Control Objective:	To ensure that the design, operation, use and management of information systems adheres to organizational security policies and standards.

Control Reference: 06.g Compliance with Security Policies and Standards

Control Specification:	Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Audit and Accountability; Documentation and Records; Policies and Procedures; Requirements (Legal and Contractual); Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	

Level 1 Regulatory Factors:	Subject to CMMC Level 2 Subject to Joint Commission Accreditation Subject to NIST 800-171 Basic Level Subject to Texas Health and Safety Code
Level 1 Implementation:	Reviews of the compliance of systems with security and privacy policies, standards and any other security and privacy requirements (HIPAA, legal, etc.) are supported by system and information owners. Compliance reviews are conducted by security, privacy and/or audit individuals and incorporate reviews of documented evidence. Automated tools are used where possible, but manual processes are acceptable. Annual compliance assessments are conducted. If any non-compliance is found as a result of the review, managers: 1. determine the causes of the non-compliance; 2. evaluate the need for actions to ensure that non-compliance does not recur; 3. determine and implement appropriate corrective action; and 4. review the corrective action taken. The results and recommendations of these reviews are documented and approved by management.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) AICPA 2017 CC2.1 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMMC v1.0 CA.2.158-0 CMSRs v3.1 AR-04 (HIGH; MOD) COBIT 5 DS5.5 COBIT 5 DSS05.07 CSA CCM v3.0.1 HRS-07 CSA CCM v3.0.1 STA-04 FFIEC IS v2016 A.10.1 FFIEC IS v2016 A.10.3(a) FFIEC IS v2016 A.10.5 FFIEC IS v2016 A.10.6 FFIEC IS v2016 A.6.4(c) FFIEC IS v2016 A.8.1(c) ISO/IEC 27002:2013 18.2.2 ISO/IEC 27002:2013 18.2.3 ISO/IEC 27799:2016 18.2.2 ISO/IEC 27799:2016 18.2.3 MARS-E v2 AR-4 NIST 800-171 r2 3.12.1-0 NIST Cybersecurity Framework v1.1 DE.DP-1 NIST Cybersecurity Framework v1.1 DE.DP-4 NIST Cybersecurity Framework v1.1 ID.RA-6 TJC IM.02.01.03, EP 8

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	

Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CMMC Level 3 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Basic Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The internal security organization regularly reviews the compliance of information processing as part of a formal risk assessment process. Automated compliance tools/scans are used where possible. The organization employs assessors or assessment teams to monitor the security controls in the information system on an ongoing basis as part of a continuous monitoring program. These teams will have a level of independence appropriate to the organization's continuous monitoring strategy. The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: 1. establishment of defined metrics to be monitored annually, at a minimum; 2. ongoing program assessments in accordance with its continuous monitoring strategy that includes, at a minimum: i. annual compliance assessments across the entire organization, and ii. third-party independent compliance assessments performed bi-annually; 3. ongoing status monitoring in accordance with its continuous monitoring strategy; 4. correlation and analysis of security-related information generated by assessments and monitoring; 5. response actions to address results of these analyses; and 6. reporting the security state of the information system to appropriate organizational officials monthly and, if required, to external agencies (e.g., HHS, CMS) as required by that agency. The security organization maintains records of the compliance results (e.g., organization-defined metrics) in order to better track security trends within the organization, respond to the results of correlation and analysis, and to address longer term areas of concern.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMMC v1.0 CA.3.161-0 CMSRs v3.1 CA-01 (HIGH; MOD) CMSRs v3.1 CA-07 (HIGH; MOD) CMSRs v3.1 CA-07(01) (HIGH; MOD) CMSRs v3.1 RA-05 (HIGH; MOD) COBIT 5 DS5.5 COBIT 5 DSS05.07 FedRAMP CA-7 FedRAMP CA-7(1) FedRAMP RA-5 FedRAMP SA-4(8) FFIEC IS v2016 A.4.1 FFIEC IS v2016 A.7.4(c) FFIEC IS v2016 A.7.4(d) FFIEC IS v2016 A.8.1(o) IRS Pub 1075 v2016 9.3.14.3

	IRS Pub 1075 v2016 9.3.4.1 IRS Pub 1075 v2016 9.3.4.6 IRS Pub 1075 v2016 Exhibit 10 ISO/IEC 27002:2013 18.2.2 ISO/IEC 27002:2013 18.2.3 ISO/IEC 27799:2016 18.2.2 ISO/IEC 27799:2016 18.2.3 MARS-E v2 CA-1 MARS-E v2 CA-7 MARS-E v2 CA-7(1) MARS-E v2 RA-5 NIST 800-171 r2 3.12.3-0 NIST Cybersecurity Framework v1.1 DE.CM-7 NIST Cybersecurity Framework v1.1 DE.DP-1 NIST Cybersecurity Framework v1.1 DE.DP-4 NIST SP 800-53 R4 CA-2(1)[HM]{0} NIST SP 800-53 R4 CA-7(1)[HM]{0} NIST SP 800-53 R4 CA-7(3)[S]{0} NIST SP 800-53 R4 CA-7[HML]{0} NIST SP 800-53 R4 PS-7e[HML]{0} NY DOH SSP v3.1 CA-2(1)[M]-0 NY DOH SSP v3.1 CA-7(1)[M]-0 NY DOH SSP v3.1 CA-7[M]-0 NY DOH SSP v3.1 CA-7a[M]-2 NY DOH SSP v3.1 CA-7b[M]-2 NY DOH SSP v3.1 CA-7e[M]-0 NY DOH SSP v3.1 CA-7f[M]-0 NY DOH SSP v3.1 CM-5(2).IS1[M]-1 NY DOH SSP v3.1 CM-8(3).IS1[M]-0 NY DOH SSP v3.1 PM-6[M]-2

Level CMS Implementation Requirements

Level CMS Implementation:	The organization employs assessors or assessment teams with CMS-CISO-defined level of independence to monitor the security controls in the information system on an ongoing basis.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	Organizations must ensure that data warehousing meets minimum security requirements defined in the current revision of NIST SP 800-53 and address the methodology used to inform management, define accountability, and address known security vulnerabilities.

Level HIX Implementation Requirements

Level HIX Implementation:	The use of independent security assessment agents or teams to monitor security controls is not required; however, if the organization employs an independent assessor or assessment teams with a CMS-defined level of independence to monitor the security controls in the information system on an ongoing basis, this can be used to satisfy security control assessment requirements.

Level PCI Implementation Requirements

Level PCI Implementation:	When being assessed as a service provider, the organization performs reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: (i) daily log reviews, (ii) firewall rule-set reviews, (iii) applying configuration standards to new systems, (iv) responding to security alerts, (v) change management processes. When being assessed as a service provider, the organization maintains documentation of quarterly review process to include: (i) documenting results of the reviews (ii) review

	and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program.

Control Reference: 06.h Technical Compliance Checking

Control Specification:	Information systems shall be regularly checked for compliance with security implementation standards. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Audit and Accountability; Requirements (Legal and Contractual); Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to Texas Health and Safety Code
Level 1 Implementation:	The organization checks the technical security configuration of information systems and network components (e.g., firewalls, routers, and switches). Checking is performed either manually, by an individual with experience with the systems, and/or with the assistance of automated software tools. These compliance checks are performed annually. If any non-compliance is found as a result of the review, the organization: 1. determines the causes of the non-compliance; 2. evaluates the need for actions to ensure that non-compliance does not recur; 3. determines and implements appropriate corrective action; and 4. reviews the corrective action taken.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CIS CSC v7.1 11.1 CIS CSC v7.1 11.3 COBIT 5 DS5.5 COBIT 5 DSS05.07 ISO/IEC 27002:2013 18.2.2 ISO/IEC 27002:2013 18.2.3 ISO/IEC 27799:2016 18.2.2 ISO/IEC 27799:2016 18.2.3 NIST Cybersecurity Framework v1.1 DE.CM-8 NIST Cybersecurity Framework v1.1 ID.RA-1 NIST Cybersecurity Framework v1.1 ID.RA-6 NIST Cybersecurity Framework v1.1 PR.IP-12 NIST Cybersecurity Framework v1.1 RS.MI-3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB)

	Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: Technical compliance checking is performed by an experienced technical specialist with the assistance of industry standard automated tools, which generate a technical report for subsequent interpretation. Deviations are logged and automatically reported. Technical compliance checks are performed at least annually, and more frequently where needed based on risk, as part of an official risk assessment process. Special attention is drawn to compliance for the purpose of technical interoperability. Mutually-agreed upon provisions and/or terms are established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence. Supply chain agreements (e.g., SLAs) between providers and customers (tenants) incorporate at least the following mutually-agreed-upon provisions and/or terms: 1. Scope of business relationship and services offered, e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations; 2. Information security requirements, provider, and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effective governance, risk management, assurance, and legal, statutory, and regulatory compliance obligations by all impacted business relationships; 3. Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts; 4. Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain); 5. Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed; 6. Expiration of the business relationship and treatment of customer (tenant) data impacted; and 7. Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence.

	Service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream) are reviewed consistently and no less than annually to identify any non-conformance to established agreements. The reviews result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships. Third-party service providers demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC4.1 CMSRs v3.1 CA-02(02) (HIGH) CMSRs v3.1 CA-07 (HIGH; MOD) CMSRs v3.1 RA-05 (HIGH; MOD) COBIT 5 DS5.5 FedRAMP CA-7 FedRAMP RA-5 IRS Pub 1075 v2016 9.3.14.3 IRS Pub 1075 v2016 9.3.4.6 ISO/IEC 27002:2013 18.2.3 ISO/IEC 27799:2016 18.2.3 MARS-E v2 CA-7 MARS-E v2 RA-5 NIST Cybersecurity Framework v1.1 DE.CM-8

Level CIS Implementation Requirements

Level CIS Implementation:	The organization utilizes an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider and update the organization's sensitive information inventory. Utilize file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The file integrity checking tools reporting system: 1. has the ability to account for routine and expected changes; 2. highlights and alerts on unusual or unexpected changes; 3. shows the history of configuration changes over time and identifies who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks also identify suspicious system alterations such as: 1. owner and permissions changes to files or directories; 2. the use of alternate data streams which could be used to hide malicious activities; 3. and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes). The organization uses an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.

Level CMS Implementation Requirements

Level CMS Implementation:	The organization includes as part of security control assessments, within every 365 days, announced or unannounced in-depth system monitoring; vulnerability scanning; malicious user testing; insider threat assessment; and performance/load testing.

Level DGF Implementation Requirements

Level DGF Implementation:	The organization has implemented tools and technologies that meet stakeholder needs to operationalize Data Governance.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The organization includes as part of its security control assessments, within every 365 days, announced vulnerability scanning.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The information system performs security compliance checks, as defined by the RMH, on constituent system components prior to the establishment of the internal connection. All applications and systems are required to undergo periodic security compliance assessments to ensure that they reflect a security posture commensurate with each SEs definition of acceptable risk. Security compliance assessments must include assessments for compliance with all federal, state, and external compliance standards for which the SE is required to comply. The organization performs automated reviews of the information system no less often than once every seventy-two [72] hours to identify changes in functions, ports, protocols, and/or services.

Objective Name: 06.03 Information System Audit Considerations

Control Objective:	Ensure the integrity and effectiveness of the information systems audit process.

Control Reference: 06.i Information Systems Audit Controls

Control Specification:	Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to, to minimize the risk of disruptions to business processes.
Factor Type:	Organizational
Topics:	Audit and Accountability; Documentation and Records; Monitoring

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1	Subject to Texas Health and Safety Code

Regulatory Factors:	
Level 1 Implementation:	At a minimum, an annual audit planning and scoping process exist and give consideration to risk, involvement of technical and business staff, other ongoing projects, and business impacts that may impact the effectiveness of the audit. If desired, a smaller quarterly process can be utilized to minimize impact to operations. The quarterly process ensures the entire organization is audited annually.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 CA-02 (HIGH; MOD) CSA CCM v3.0.1 AAC-02 FedRAMP CA-2 IRS Pub 1075 v2016 9.3.4.2 ISO/IEC 27002:2013 12.7.1 ISO/IEC 27799:2016 12.7.1 MARS-E v2 CA-2 NIST Cybersecurity Framework v1.1 DE.DP-1 NIST Cybersecurity Framework v1.1 DE.DP-2 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 PR.PT-1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The organization develops, disseminates, and reviews/updates annually: 1. a formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. While planning and performing operational system audits, the following are addressed: 1. audit requirements are agreed upon with appropriate management, but at a minimum address user access and behavior risks; 2. the scope of the checks is agreed and controlled; 3. the checks are limited to read-only access to software and data;

	4. access other than read-only is only allowed for isolated copies of system files, which are erased when the audit is completed; 5. IT resources for performing the checks are explicitly identified and made available; 6. requirements for special or additional processing are identified and agreed; 7. all access is monitored and logged to produce a reference trail; 8. all procedures, requirements and responsibilities are documented; 9. the person(s) carrying out the audit are independent of the activities audited; 10. scheduling of the audits is performed during times of least impact to business operations, for example, not during other audits such as financial audits, end of major financial periods, deployments of major systems, etc.; and 11. audits are scheduled in advance to ensure availability of proper individuals and systems, and coordination of all business units.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC3.1 AICPA 2017 CC5.1 CMSRs v3.1 AU-01 (HIGH; MOD) CMSRs v3.1 PL-02 (HIGH; MOD) CSA CCM v3.0.1 AAC-01 FedRAMP AU-1 FedRAMP PL-2 IRS Pub 1075 v2016 9.3.12.2 IRS Pub 1075 v2016 9.3.3.1 ISO/IEC 27002:2013 12.7.1 ISO/IEC 27799:2016 12.7.1 MARS-E v2 AU-1 MARS-E v2 PL-2 NIST Cybersecurity Framework v1.1 DE.DP-1 NIST Cybersecurity Framework v1.1 DE.DP-2 NIST Cybersecurity Framework v1.1 DE.DP-4 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 PR.PT-1 PMI DSP Framework DE-1

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The organization determines, based on a risk assessment and CMS mission/business needs, that the information system can audit the predefined list of auditable events. The organization determines which pre-defined auditable events require auditing on a continuous basis in response to specific situations. The organization determines that the information system can audit privileged activities or system level access to PII. The organization determines that the information system can audit concurrent logons from different workstations. The organization determines that privileged activities or system level access to PII is audited within the information system. The organization determines that concurrent logons from different workstations is audited within the information system. The organization reviews and updates the list of auditable events no less often than every three hundred sixty-five [365] days and whenever there is a significant system modification. The information system takes actions in response to an audit failure or audit storage capacity issue. The organization reviews system records for initialization sequences, logons (successful and unsuccessful), errors, system processes, security software (e.g., malicious code protection, intrusion detection, firewall), applications, performance, and system resource

	utilization to determine anomalies no less often than once within a twenty-four [24] hour period and on demand. Generate alert notification for technical personnel review and assessment. The organization uses automated utilities to review audit records no less often than once every seventy-two [72] hours for unusual, unexpected, or suspicious behavior. The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. The organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information. The information system provides audit record generation capability for all changes to logical access control authorities (e.g., rights, permissions).

Control Reference: 06.j Protection of Information Systems Audit Tools

Control Specification:	Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.
Factor Type:	Organizational
Topics:	Audit and Accountability; Authorization; User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to Supplemental Requirements
Level 1 Implementation:	Access to information systems audit tools is protected to prevent any possible misuse or compromise.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 AU-09 (HIGH; MOD) CSA CCM v3.0.1 IAM-01 FedRAMP AU-9 IRS Pub 1075 v2016 9.3.3.10 MARS-E v2 AU-9 NIST Cybersecurity Framework v1.1 DE.DP-1 NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.AC-4 SR v6.4 31-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions

	Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to CMMC Level 3 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (Supplemental) Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: Information systems audit tools (e.g., software or data files) are separated from development and operational systems and not held in tape libraries or user areas. Access to these tools is documented and enforced per a formal procedure, restricted to authorized individuals only, and approved by designated system owners. Use of these tools is only authorized after receiving permission from system owners and as part of a documented assessment process. Specific controls identified within the access control section are also enforced for the audit tools. Audits of these controls are performed at least annually.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMMC v1.0 AU.3.050-0 CMSRs v3.1 AC-06(01) (HIGH; MOD) CMSRs v3.1 AU-01 (HIGH; MOD) CMSRs v3.1 AU-02 (HIGH; MOD) CMSRs v3.1 AU-09 (HIGH; MOD) CMSRs v3.1 CA-02 (HIGH; MOD) CSA CCM v3.0.1 AAC-02 FedRAMP AC-6(1) FedRAMP AU-1 FedRAMP AU-9 FedRAMP CA-2 IRS Pub 1075 v2016 9.3.3.10 IRS Pub 1075 v2016 9.3.3.11 IRS Pub 1075 v2016 9.3.4.2 ISO/IEC 27002:2013 12.7.1 ISO/IEC 27799:2016 12.7.1 MARS-E v2 AC-6(1) MARS-E v2 AU-1 MARS-E v2 AU-9 MARS-E v2 CA-2 NIST 800-171 r2 3.3.9-0 NIST Cybersecurity Framework v1.1 DE.DP-1 NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.IP-1 NIST Cybersecurity Framework v1.1 PR.PT-3 NIST SP 800-53 R4 AU-9(5)[S]{2}

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The organization authorizes access to management of audit functionality to only those individuals or roles who are not subject to audit by that system and is defined in the applicable system security plan. The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

Control Category: 07.0 - Asset Management

Objective Name: 07.01 Responsibility for Assets

Control Objective:	To ensure that management requires ownership and defined responsibilities for the protection of information assets.

Control Reference: 07.a Inventory of Assets

Control Specification:	All assets including information shall be clearly identified and an inventory of all assets drawn up and maintained. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Contingency Planning; Documentation and Records; IT Organization and Management Roles and Responsibilities; Media and Assets; Third-parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 2 Subject to HIPAA Security Rule Subject to HITRUST De-ID Framework Requirements Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Privacy) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Texas Health and Safety Code
Level 1 Implementation:	The organization identifies and inventories all assets and services including information (e.g., PII), encrypted or unencrypted, wherever it is created, received, maintained, or transmitted, including organizational and third-party sites, and documents the importance of these assets. Locations in which PII constitutes a designated record set are explicitly identified in the asset inventory. Approved bring your own device (BYOD) equipment is also included on the organizations inventories. The asset inventories also include all information necessary to recover from a disaster, including type or classification of the asset, format, location, backup information, license information, and the importance of these assets (business value). The inventory does not duplicate other inventories unnecessarily, but it is ensured that the content is aligned. The organization maintains an inventory of authorized wireless access points, including a documented business justification, to support unauthorized WAP identification (see 09.m) and response (see 11.c). Specific policies exist for maintaining records of organizational property (capital and non-capital) assigned to employees, contractors, or volunteers. Organization management is

	responsible for establishing procedures to issue and inventory property assigned to employees. Records of property assigned to employees are reviewed and updated annually. The record is used to document and ensure that all property is returned to the organization upon employee termination or transfer out of the organization or department. Organizations that assign organization-owned property to contractors ensure that the procedures for assigning and monitoring the use of the property are included in the contract. If organization-owned property is assigned to volunteer workers, there is a written agreement specifying how and when the property will be inventoried and how it is returned upon completion of the volunteer assignment. The organization creates and documents the process/procedure the organization intends to use for deleting data from hard-drives prior to property transfer, exchange, or disposal/surplus. The organization creates and documents the process/procedure the organization intends to use to transfer, exchange or dispose of an IT-related asset (according to the organization's established lifecycle). If dynamic host configuration protocol (DHCP) is used to dynamically assign IP addresses, ensure the DHCP server logs are used to help detect unknown systems on the network and improve the organization's asset inventory. The asset inventory includes all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory includes every system that has an Internet protocol (IP) address on the network including, but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.310(d)(2)(iii) HIPAA.SR-2 AICPA 2017 CC6.1 AICPA 2017 CC6.5 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CIS CSC v7.1 1.4 CIS CSC v7.1 1.5 CIS CSC v7.1 15.1 CMMC v1.0 AC.2.011-2 CMSRs v3.1 CM-08(05) (HIGH; MOD) CMSRs v3.1 MP-01 (HIGH; MOD) CMSRs v3.1 PM-05 (HIGH; MOD) COBIT 5 APO12.03 CRR v2016 AM:G2.Q1 CRR v2016 AM:G2.Q5 CRR v2016 AM:G3.Q1 CRR v2016 AM:G6.Q6 CRR v2016 AM:G6.Q7 CRR v2016 AM:MIL2.Q1 CRR v2016 AM:MIL2.Q2 CRR v2016 AM:MIL2.Q4 CSA CCM v3.0.1 DCS-01 CSA CCM v3.0.1 MOS-09 De-ID Framework v1 Data Storage: General FedRAMP CM-8(5) FedRAMP MP-1 FFIEC IS v2016 A.6.16(a) FFIEC IS v2016 A.6.16(e) FFIEC IS v2016 A.6.6

	HITRUST IRS Pub 1075 v2016 9.3.10.1 IRS Pub 1075 v2016 9.4.12 ISO/IEC 27002:2013 8.1.1 ISO/IEC 27799:2016 8.1.1 MARS-E v2 MP-1 MARS-E v2 PM-5 NIST 800-171 r2 3.1.16-2 NIST Cybersecurity Framework v1.1 ID.AM-1 NIST Cybersecurity Framework v1.1 ID.AM-2 NIST Cybersecurity Framework v1.1 ID.AM-5 NIST Cybersecurity Framework v1.1 PR.DS-3 NIST SP 800-53 R4 CM-8(7)[S]{0} NIST SP 800-53 R4 CM-8a[HML]{1} NIST SP 800-53 R4 PE-20a[S]{0} NIST SP 800-53 R4 SA-19(3)[S]{0} NIST SP 800-53 R4 SE-1[P]{0} NIST SP 800-53 R4 SI-13(3)[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 CM-8(5)[M]-0 PCI DSS v3.2.1 11.1.1 PCI DSS v3.2.1 12.3.3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Community Supplemental Requirements 002 Subject to HIPAA Security Rule Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance
Level 2 Implementation:	Level 1 plus: Ownership, custodianship, and information classification are agreed and documented for each of the assets. Based on the importance of the asset, its business value and its security classification, levels of protection and sustainment commensurate with the importance of the assets are identified. The organization maintains inventory logs of all media and conduct media inventories at least annually.
Level 2 Control Standard Mapping:	45 CFR Part § 164.310(d)(1) HIPAA.SR-2 AICPA 2017 CC6.1 CRR v2016 AM:G6.Q1 CSR002 v2018 11.2-4-2 FFIEC IS v2016 A.6.6 ISO/IEC 27002:2013 8.1.1 ISO/IEC 27799:2016 8.1.1 NIST Cybersecurity Framework v1.1 ID.AM-5 NIST SP 800-53 R4 CM-8a[HML]{2}

	NRS 603A.215.1 NY DOH SSP v3.1 AC-20(3)a[MN]-0 NY DOH SSP v3.1 CM-8a3[M]-0 PCI DSS v3.2.1 2.4 PCI DSS v3.2.1 9.7.1 PCI DSS v3.2.1 9.9 PCI DSS v3.2.1 9.9.1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to Banking Requirements Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 2 Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to HIPAA Security Rule Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Basic Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: The organization creates, documents, and maintains a process and procedure to physically inventory and reconciles IT asset inventory information on hand for: 1. Capital Assets (Inventory must be conducted at least annually); and 2. Non-Capital Assets. The asset inventory includes: 1. Unique identifier and/or serial number; 2. Information system of which the component is a part; 3. Type of information system component (e.g., server, desktop, application); 4. Manufacturer/model information; 5. Operating system type and version/service pack level; 6. Presence of virtual machines; 7. Application software version/license information; 8. Physical location (e.g., building/room number); 9. Logical location (e.g., IP address, position with the IS architecture); 10. Media access control (MAC) address; 11. Data ownership and custodian by position and role;

12. Operational status;
13. Primary and secondary administrators;
14. Primary user; and
15. Mapped organizational communications and data flows.

The organization:

1. employs automated mechanisms to scan the network no less than weekly to detect the presence of unauthorized components/devices (including hardware, firmware, and software) into the information system; and
2. disables network access by such components/devices and notify designated organizational officials.

The organization implements an IT Asset Lifecycle Program, and monitors its effectiveness, making changes as needed. The organization implements six stages for the lifecycle of an IT Asset. The following activities for each stage include:

1. planning - defining supporting processes, setting standards for configuration and retention, aligning purchase plans to business goals, collecting aggregate information on intended purchases, and negotiating volume discounts;
2. procurement - requisitioning, approving requisitions, ordering, receiving, and validating orders;
3. deployment - tagging assets, entering asset information in a repository, configuring, and installing assets including:
    i. disabling unnecessary or insecure services or protocols,
    ii. limiting servers to one primary function, and
    iii. defining system security parameters to prevent misuse;
4. management - inventory/counting, monitoring usage (some software), managing contracts for maintenance and support, and monitoring age and configuration;
5. support - adding and changing configurations, repairing devices, and relocating equipment and software; and
6. disposition - removing assets from service, deleting storage contents, disassembling components for reuse, surplusage equipment, terminating contracts, disposing of equipment, and removing assets from active inventory.

The organization provides each update of the inventory identifying assets with covered information (e.g., PII) to the CIO or information security official, and the senior privacy official on an organization-defined basis, but no less than annually, to support the establishment of information security requirements for all new or modified information systems containing this information.

Level 3 Control Standard Mapping:

1 TAC § 390.2(a)(4)(A)(xi)
45 CFR Part § 164.310(d)(2)(iii) HIPAA.SR-3
AICPA 2017 CC7.1
CMMC v1.0 CM.2.061-2
CMSRs v3.1 CM-08 (HIGH; MOD)
CMSRs v3.1 CM-08(01) (HIGH; MOD)
CMSRs v3.1 CM-08(02) (HIGH)
CMSRs v3.1 CM-08(03) (HIGH; MOD)
CMSRs v3.1 CM-08(04) (HIGH)
CMSRs v3.1 CM-08(05) (HIGH; MOD)
CMSRs v3.1 PM-05 (HIGH; MOD)
CMSRs v3.1 SE-01 (HIGH; MOD)
CRR v2016 AM:G2.Q3
CRR v2016 AM:G2.Q4
CRR v2016 AM:G4.Q2
CRR v2016 VM:G1.Q5
FedRAMP CM-7
FedRAMP CM-8
FedRAMP CM-8(1)
FFIEC IS v2016 A.6.16(b)
FFIEC IS v2016 A.6.16(c)
FFIEC IS v2016 A.6.16(d)
IRS Pub 1075 v2016 4.5
IRS Pub 1075 v2016 9.3.5.8

	IRS Pub 1075 v2016 9.4.12 IRS Pub 1075 v2016 9.4.18 MARS-E v2 CM-8 MARS-E v2 CM-8(1) MARS-E v2 PM-5 MARS-E v2 SE-1 NIST 800-171 r2 3.4.1-2 NIST Cybersecurity Framework v1.1 ID.AM-1 NIST Cybersecurity Framework v1.1 ID.AM-2 NIST Cybersecurity Framework v1.1 PR.DS-3 NIST SP 800-53 R4 CM-11(1)[S]{0} NIST SP 800-53 R4 CM-8(1)[HM]{0} NIST SP 800-53 R4 CM-8(3)[HM]{0} NIST SP 800-53 R4 CM-8b[HML]{1} NIST SP 800-53 R4 PM-5[HML]{2} NIST SP 800-53 R4 SA-10(6)[S]{2} NIST SP 800-53 R4 SA-19(4)[S]{0} NIST SP 800-53 R4 SA-19[S]{0} NIST SP 800-53 R4 SC-7(14)[S]{0} NIST SP 800-53 R4 SI-13(1)[S]{0} NIST SP 800-53 R4 SI-4(22)[S]{0} NY DOH SSP v3.1 CM-8(1)[M]-0 NY DOH SSP v3.1 CM-8(3)a[M]-0

Level CIS Implementation Requirements

Level CIS Implementation:	The organization deploys active and passive automated asset discovery tool(s) and uses it to build/maintain/reconcile an asset inventory of systems connected to its public and private network(s). The organization uses dynamic host configuration protocol (DHCP) logging on all DHCP or IP address management tools to improve the organization's asset inventory. The organization uses a software inventory system tool to automate the documentation of all software on business systems, tracking the name, version, publisher, and install date for all software, including operating systems unauthorized by the organization.

Level CMS Implementation Requirements

Level CMS Implementation:	The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components. The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories. In addition to the creation of the IT Asset Lifecycle Program, the organization identifies an owner to manage all organization IT asset inventory and management-related process and procedure documents. This owner ensures that the IT Asset Lifecycle Program: 1. identifies and documents personnel with IT asset roles and responsibilities; 2. provides procurement training to personnel with IT asset roles and responsibilities; 3. provides procurement training material addressing the procedures and activities necessary to fulfill IT asset roles and responsibilities; 4. defines the frequency of refresher training; and 5. provides refresher IT asset training in accordance with organization defined frequency, at least on an annual basis.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The organization employs automated mechanisms to scan the network continuously with a maximum 5-minute delay in detection to detect the presence of unauthorized components/devices (including hardware, firmware and software) into the information system; and disable network access by such components/devices and notify designated organizational officials.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The organization develops and documents an inventory of information system components that includes: (i) Each component's unique identifier and/or serial number; (ii) Information system of which the component is a part; (iii) Type of information system component (e.g., server, desktop, application); (iv) Manufacturer/model information; (v) Operating system type and version/service pack level; (vi) Presence of virtual machines; (vii) Application software version/license information; (xiii) Physical location (e.g., building/room number); (ix) Logical location (e.g., IP address, position with the information system [IS] architecture); (x) Media access control (MAC) address; (xi) Ownership; (xii) Operational status; (xii) Primary and secondary administrators; and (xiii) Primary user. Fully integrate inventory of information system components with the organizational continuous monitoring capability. The organization removes previous versions of software and/or firmware components after updated versions have been installed.

Level PCI Implementation Requirements

Level PCI Implementation:	The organization maintains an inventory of system components that are in scope for PCI DSS. Lists of payment card devices are kept up to date and include the following: 1. Make and model of device; 2. Location of device (for example, the address of the site or facility where the device is located); 3. Device serial number or other method of unique identification. The inventory of system components and devices in scope for PCI DSS identifies all personnel authorized to use the system components and devices.

Control Reference: 07.b Ownership of Assets

Control Specification:	All information and assets associated with information processing systems shall be owned by a designated part of the organization.
Factor Type:	Organizational
Topics:	IT Organization and Management Roles and Responsibilities; Media and Assets

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	

Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance
Level 1 Implementation:	All information systems are documented including a method to accurately and readily determine the assigned owner of responsibility, contact information, and purpose (e.g., through labeling, coding, and/or inventory).
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC6.1 CMSRs v3.1 CM-08 (HIGH; MOD) CRR v2016 AM:MIL2.Q4 CSA CCM v3.0.1 DCS-01 CSA CCM v3.0.1 DSI-06 FedRAMP CM-7 FedRAMP CM-8 IRS Pub 1075 v2016 9.3.5.8 MARS-E v2 CM-8 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST SP 800-53 R4 CM-8(9)a[S]{0} NIST SP 800-53 R4 PM-5[HML]{1} NRS 603A.215.1 NY DOH SSP v3.1 CM-8(4)[HN]-0 NY DOH SSP v3.1 PM-5[M]-0 PCI DSS v3.2.1 12.3.4

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CMMC Level 3 Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus:

	The asset owner (e.g., individual responsible) is responsible for: 1. ensuring that information and assets associated with information processing systems are appropriately classified; and 2. defining and periodically (at a minimum, annually) reviewing access restrictions and classifications, taking into account applicable access control policies. Responsibility may be allocated to: 1. a business process; 2. a defined set of activities; 3. an application; or 4. a defined set of data. The organization creates and documents the process/procedures the organization intends to use to ensure that appropriate software licensing agreements for software used by organization employees are in place and that the organization is in compliance with those agreements. All information and assets associated with information processing systems are assigned responsibility to a designated part of the organization. All information has an information owner or owners (e.g., designated individuals responsible) established within the organization's lines of business. The information owner(s) are responsible to: 1. create an initial information classification, including assigning classification levels to all data; 2. approve decisions regarding controls, access privileges of users, and ongoing decisions regarding information management; 3. ensure the information will be regularly reviewed for value and updates to manage changes to risks due to new threats, vulnerabilities, or changes in the environment; 4. perform, on an organization pre-defined time frame, reclassification based upon business impact analysis, changing business priorities and/or new laws, regulations, and security standards; and 5. follow organization's archive document retention rules regarding proper disposition of all information assets. When a person(s) designated as information owner no longer has the responsibility due to departure, transfer or reassignment, the organization appoints a new information owner(s) in a timely manner to ensure no lapse in accountability and responsibility for information assets.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMMC v1.0 MP.3.123-1 CMSRs v3.1 CM-08 (HIGH; MOD) CMSRs v3.1 CM-10 (HIGH; MOD) CRR v2016 AM:G2.Q3 CRR v2016 AM:G5.Q1 CRR v2016 AM:G5.Q2 CRR v2016 AM:G5.Q3 CRR v2016 AM:G5.Q4 CSA CCM v3.0.1 DCS-01 CSA CCM v3.0.1 DSI-06 FedRAMP CM-10 FedRAMP CM-7 FFIEC IS v2016 A.6.6 IRS Pub 1075 v2016 9.3.5.10 IRS Pub 1075 v2016 Exhibit 10 ISO/IEC 27002:2013 8.1.2 ISO/IEC 27799:2016 8.1.2 MARS-E v2 CM-8 NIST 800-171 r2 3.8.8-1 NIST Cybersecurity Framework v1.1 ID.AM-5 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 ID.GV-3

	NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 PR.DS-3 NIST SP 800-53 R4 CM-10a[HML]{0} NIST SP 800-53 R4 CM-8(9)b[S]{0} NIST SP 800-53 R4 PS-3(2)[S]{2} NY DOH SSP v3.1 CM-10a[M]-0

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	All FTI have a management official, e.g., an accrediting authority, assigned as an owner to provide responsibility and accountability for its protection. The agency configures control files and data sets to enable the FTI data owner to analyze and review both authorized and unauthorized accesses to a data warehouse.

Control Reference: 07.c Acceptable Use of Assets

Control Specification:	Rules for the acceptable use of information and assets associated with information processing systems shall be identified, documented, and implemented. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Awareness and Training; Documentation and Records; Media and Assets; Personnel

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 3 Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to Joint Commission Accreditation Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to State of Massachusetts Data Protection Act Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	The organization establishes and makes readily available to all information system users, a set of rules that describe their responsibilities and expected behavior with regards to information and information system usage. Employees, contractors and third-party users using or having access to the organization's assets are aware of the limits existing for their use of the organization's information and assets associated with information processing facilities, and resources. They are responsible for their use of any information processing resources, and of any such use carried out under their responsibility. Acceptable use addresses: 1. rules for electronic mail and Internet usages; and

	2. guidelines for the use of mobile devices, especially for the use outside the premises of the organization. The organization includes in the rules of behavior, explicit restrictions on the use of social media and networking sites, posting information on commercial websites, and sharing information system account information.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 201 CMR 17.03(2)(c) CMMC v1.0 SC.3.193-2 CMSRs v3.1 AC-20 (HIGH; MOD) CMSRs v3.1 PL-04 (HIGH; MOD) CMSRs v3.1 PL-04(01) (HIGH; MOD) CSA CCM v3.0.1 HRS-08 FedRAMP AC-20 FedRAMP PL-4 FedRAMP PL-4(1) FFIEC IS v2016 A.6.18(g) FFIEC IS v2016 A.6.8(f) IRS Pub 1075 v2016 9.3.12.3 ISO/IEC 27002:2013 8.1.3 ISO/IEC 27799:2016 8.1.3 MARS-E v2 AC-20 MARS-E v2 PL-4 MARS-E v2 PL-4(1) NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 PR.AT-1 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST SP 800-53 R4 PL-4(1)[HM]{0} NIST SP 800-53 R4 PL-4a[HML]{0} NRS 603A.215.1 NY DOH SSP v3.1 PL-4(1)[M]-0 NY DOH SSP v3.1 PL-4a[M]-0 NY DOH SSP v3.1 PL-4a1[M]-0 NY DOH SSP v3.1 PL-4a2[M]-0 NY DOH SSP v3.1 PL-4a3[M]-0 PCI DSS v3.2.1 12.3 PCI DSS v3.2.1 12.3.5 TJC IM.02.01.03, EP 1

Objective Name: 07.02 Information Classification

Control Objective:	To ensure that information receives an appropriate and consistent level of protection.

Control Reference: 07.d Classification Guidelines

Control Specification:	Information shall be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.
Factor Type:	Organizational
Topics:	Audit and Accountability; IT Organization and Management Roles and Responsibilities; Media and Assets

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1	Subject to FISMA Compliance

Regulatory Factors:	
Level 1 Implementation:	Organizations processing PII uniformly classify such data as confidential, which means that there are limitations to its disclosure within the organization and externally.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) NIST Cybersecurity Framework v1.1 ID.AM-5 NIST Cybersecurity Framework v1.1 PR.DS-5

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to Community Supplemental Requirements 002 Subject to CRR V2016 Subject to FedRAMP Certification Subject to IRS Pub 1075 Compliance Subject to Joint Commission Accreditation Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The organization categorizes (classify) records by type (e.g., accounting records, database records, transaction logs, audit logs and operational procedures) with details of storage media and documents the results. Classifications and associated protective controls for information take account of: 1. business needs for sharing or restricting information; 2. the business impacts associated with such needs; and 3. the form of the data, such as raw, aggregate (see 09.p), the product of a mathematical or statistical process or an analysis report. Classification guidelines include conventions for initial classification and reclassification over time in accordance with the access control policy. It is the responsibility of the asset owner (see 7.b) to: 1. define the classification of an asset; 2. periodically review the classification; 3. ensure it is kept up to date; and

	4. ensure it is at the appropriate level. Consideration is given to the number of classification categories and the benefits to be gained from their use. Overly complex schemes can become cumbersome and uneconomic to use or prove impractical. The level of protection is assessed by analyzing confidentiality, integrity and availability and any other requirements for the information considered, including whether or not the information requires the application of encryption to address confidentiality and integrity requirements (see also 01.x, 06.d and 09.y). Organizations identify, record, and control inventory items that have a high risk of loss such as computer and electronic equipment and hand tools and instruments. Personal property meeting the definition of capital assets is capitalized, tagged with an organization identification tag and property control number, listed on the capital asset property inventory, and physically inventoried at least annually. Discrepancies are investigated. Documentation that a physical inventory has been taken, for all locations, is retained in the organization's central accounting office. The organization creates and documents process and procedure to affix an organization identification tag to: 1. newly purchased IT-related assets (Tagging required prior to deployment in the computing environment); 2. existing non-capital assets (Tagging required within one year); and 3. existing capital assets (Tagging required within one year). Care is taken in interpreting classification labels on documents from other organizations, which may have different definitions for the same or similarly named labels. The organization documents security categorizations (including supporting rationale) in the security plan for the information system.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 CM-08 (HIGH; MOD) CMSRs v3.1 RA-02 (HIGH; MOD) CRR v2016 AM:G3.Q2 CRR v2016 AM:G6.Q1 CRR v2016 AM:G6.Q2 CRR v2016 RM:G2.Q1 CSA CCM v3.0.1 DSI-01 CSR002 v2018 11.2-4-1 FedRAMP CM-7 FedRAMP CM-8 FedRAMP RA-2 FFIEC IS v2016 A.6.6 HITRUST IRS Pub 1075 v2016 Exhibit 10 ISO/IEC 27002:2013 8.1.1 ISO/IEC 27002:2013 8.1.2 ISO/IEC 27002:2013 8.2.1 ISO/IEC 27799:2016 ISO/IEC 27799:2016 8.1.1 ISO/IEC 27799:2016 8.1.2 ISO/IEC 27799:2016 8.2.1 MARS-E v2 CM-8 MARS-E v2 RA-2 NIST Cybersecurity Framework v1.1 ID.AM-1 NIST Cybersecurity Framework v1.1 ID.AM-2 NIST Cybersecurity Framework v1.1 ID.AM-5 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST Cybersecurity Framework v1.1 ID.RA-3 NIST Cybersecurity Framework v1.1 ID.RA-4 NIST Cybersecurity Framework v1.1 ID.RA-5

	NIST Cybersecurity Framework v1.1 IR.RA-4 NIST Cybersecurity Framework v1.1 PR.DS-3 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST SP 800-53 R4 AC-16(1)[S]{0} NIST SP 800-53 R4 AC-16(10)[S]{1} NIST SP 800-53 R4 AC-16(10)[S]{2} NIST SP 800-53 R4 AC-16(2)[S]{1} NIST SP 800-53 R4 AC-16(3)[S]{0} NIST SP 800-53 R4 AC-16(4)[S]{0} NIST SP 800-53 R4 AC-16(6)[S]{0} NIST SP 800-53 R4 AC-16(7)[S]{2} NIST SP 800-53 R4 AC-16(8)[S]{2} NIST SP 800-53 R4 AC-16(9)[S]{0} NIST SP 800-53 R4 PL-8a[HM]{2} NIST SP 800-53 R4 PM-11b[HML]{0} NIST SP 800-53 R4 RA-2a[HML]{0} NIST SP 800-53 R4 RA-2b[HML]{0} NY DOH SSP v3.1 CM-8.IS1[M]-0 NY DOH SSP v3.1 CM-8.IS2[M]-1 NY DOH SSP v3.1 CM-8.IS2[M]-2 NY DOH SSP v3.1 RA-2a[M]-0 NY DOH SSP v3.1 RA-2b[M]-0 PMI DSP Framework ID-2 TJC IM.02.01.03, EP 5

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to Banking Requirements Subject to NIST SP 800-53 R4 (Supplemental)
Level 3 Implementation:	Level 2 plus: Organizations establish a classification schema to differentiate between various levels of sensitivity and value. Information assets are classified according to their level of sensitivity as follows: • Level 1: Low-sensitive information. Information that is not protected from disclosure, that if disclosed will not jeopardize the privacy or security of employees, clients, and partners. This includes information regularly made available to the public via electronic, verbal or hard copy. • Level 2: Sensitive information that may not to be protected from public disclosure, but if made easily and readily available, the organization follows its disclosure policies and procedures before providing this information to external parties. • Level 3: Sensitive information intending for limiting business use that can be exempt from public disclosure because, among other reasons, such disclosure will jeopardize the privacy or security of employees, clients, or partners. • Level 4: Information that is deemed extremely sensitive and is intended for use by named individuals only. This information is typically exempt from public disclosure. Users of information systems are notified and made aware when the data they are accessing contains PII.

Level 3 Control Standard Mapping:	FFIEC IS v2016 A.6.6 HITRUST ISO/IEC 27002:2013 8.2.1 ISO/IEC 27799:2016 8.2.1 NIST Cybersecurity Framework v1.1 ID.AM-5 NIST Cybersecurity Framework v1.1 ID.GV-4 NIST SP 800-53 R4 AC-16d[S]{0}

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	Access controls in a data warehouse are classified in general as follows: 1. General users; 2. Limited access users; and 3. Unlimited access users. FTI always fall into the limited access user's category.

Control Reference: 07.e Information Labeling and Handling

Control Specification:	An appropriate set of procedures for information labeling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.
Factor Type:	Organizational
Topics:	Media and Assets

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to State of Massachusetts Data Protection Act Subject to Texas Health and Safety Code
Level 1 Implementation:	Organizations physically and/or electronically label and handle sensitive information commensurate with the risk of the information or document. Care is given to ensure client/customer information subject to special handling is identified and appropriate labeling and handling requirements are expressly defined and implemented consistent with applicable federal and state legislative and regulatory requirements and industry guidelines. The labeling reflects the classification according to the rules in the information classification policy. Items to include are printed reports, screen displays, recorded media (e.g., tapes, disks, CDs, electronic messages, and file transfers). The organization may exempt specific types of media or hardware components, as specified, in writing, by the CIO or his/her designated representative, from marking as long as the exempted items remain within a secure environment.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(ii) 1 TAC § 390.2(a)(4)(A)(vi) 1 TAC § 390.2(a)(4)(A)(vii) 1 TAC § 390.2(a)(4)(B)(iv) 201 CMR 17.03(2)(g) AICPA 2017 C1.1

	CMSRs v3.1 MP-03 (HIGH; MOD) CRR v2016 AM:G6.Q3 CSA CCM v3.0.1 DSI-04 FedRAMP MP-3 HITRUST MARS-E v2 MP-3 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.PT-2 NIST SP 800-53 R4 AC-16(5)[S]{1} NIST SP 800-53 R4 AC-4(18)[S]{0} NY DOH SSP v3.1 MP-3b[M]-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to CRR V2016 Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (Supplemental) Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: Procedures for information labeling cover information assets in physical and electronic formats, supported by automated tools. Output from systems containing information that is classified as being sensitive or critical carries an appropriate classification label (in the output). For each classification level, handling procedures including the secure processing, storage, transmission, declassification, and destruction are defined. This also includes the procedures for chain of custody and logging of any security relevant event. Agreements with other organizations that include information sharing include procedures to identify the classification of that information and to interpret the classification labels from other organizations.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 C1.2 CMSRs v3.1 MP-03 (HIGH; MOD) CRR v2016 AM:G6.Q3 FedRAMP MP-3 IRS Pub 1075 v2016 9.3.10.3 IRS Pub 1075 v2016 9.4.3 IRS Pub 1075 v2016 9.4.4 ISO/IEC 27002:2013 16.1.7 ISO/IEC 27002:2013 8.2.2 ISO/IEC 27002:2013 8.2.3 ISO/IEC 27799:2016 16.1.7 ISO/IEC 27799:2016 8.2.2 ISO/IEC 27799:2016 8.2.3 MARS-E v2 MP-3

	NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.PT-2 NIST SP 800-53 R4 AC-16(7)[S]{1} NIST SP 800-53 R4 AC-16a[S]{0} NIST SP 800-53 R4 AC-16c[S]{0} NIST SP 800-53 R4 PE-5(3)[S]{0} NRS 603A.215.1 PCI DSS v3.2.1 9.6.1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to FedRAMP Certification
Level 3 Implementation:	Level 2 plus: Information belonging to different classification levels is logically or physically separated. Whenever possible, information assets classified as "Critical" are stored in a separate, secure area. All information systems processing covered information (e.g., PII) inform users of the confidentiality of covered information accessible from the system (e.g., at start-up or log-in).
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 AC-08 (HIGH; MOD) FedRAMP AC-8 IRS Pub 1075 v2016 9.3.1.8 MARS-E v2 AC-8 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.PT-2

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	The agency must label removable media and information system output containing FTI to indicate the distribution limitations and handling caveats (note IRS Notice 129-A or Notice 129-B are available for this purpose). Properly label emails that contain FTI (e.g., email subject contains 'FTI') to ensure that the recipient is aware that the message content contains FTI. The agency includes a cover sheet on fax transmissions that explicitly provides guidance to the recipient, which includes: 1. A notification of the sensitivity of the data and the need for protection; and 2. ii. A notice to unintended recipients to telephone the sender - collect, if necessary - to report the disclosure and confirm destruction of the information.

Level HIPAA Implementation Requirements

Level HIPAA Implementation:	Care is given to ensure patient information subject to special handling, e.g., HIV test results and mental health and substance abuse-related records, is identified and appropriate labeling and handling requirements are expressly defined and implemented consistent with applicable federal and state legislative and regulatory requirements and industry guidelines.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation:	If Personally Identifiable Information (PII) or Protected Health Information (PHI) is allowed to be included with fax communications, the organization establishes policies and procedures for handling fax transmissions.

Level Texas Covered Entities Implementation Requirements	
Level Texas Covered Entities Implementation:	Freestanding emergency medical facilities implement the Health and Human Services Executive Commissioner's minimum standards for the contents, maintenance, and release of medical records and designate an individual to be in charge of the creation, maintenance and disposal of medical records per TAC § 131.53, including the confidentiality, security and safe storage of medical records throughout the record's life cycle.

Control Category: 08.0 - Physical and Environmental Security

Objective Name: 08.01 Secure Areas

Control Objective:	To prevent unauthorized physical access, damage, and interference to the organization's premises and information.

Control Reference: 08.a Physical Security Perimeter

Control Specification:	Security perimeters (barriers such as walls, card-controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information assets.
Factor Type:	Organizational
Topics:	Authorization; Physical and Facility Security; Third-parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to HIPAA Security Rule Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Texas Health and Safety Code
Level 1 Implementation:	Computers that store or process covered and/or confidential information are not located in areas that are unattended and have unrestricted access by the public. These computers are located in rooms with doors and windows that are locked when unattended and external protection considered for windows, particularly at ground level (public, sensitive, and restricted areas). Physical barriers, where applicable, are built to prevent unauthorized physical access and environmental contamination (sensitive and restricted areas). Any repairs or modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks) are authorized by management, documented and the documentation retained in accordance with the organization's retention policy. Perimeters of a building or site containing information assets are physically sound; there are no gaps in the perimeter or areas where a break-in could easily occur. The external walls of the site are of solid construction and all external doors are protected against unauthorized access with control mechanisms (e.g., bars, alarms, locks etc.).
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.310(c) HIPAA.SR-2 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 MA-02 (HIGH; MOD) COBIT 5 DSS05.05

	CSA CCM v3.0.1 DCS-02 De-ID Framework v1 Public Access to Sensitive Areas: General FedRAMP MA-2 FFIEC IS v2016 A.6.21(c) FFIEC IS v2016 A.6.8 IRS Pub 1075 v2016 9.3.9.2 ISO/IEC 27002:2013 11.1.1 ISO/IEC 27002:2013 11.2.6 ISO/IEC 27799:2016 11.1.1 ISO/IEC 27799:2016 11.2.6 MARS-E v2 MA-2 NIST Cybersecurity Framework v1.1 DE.CM-2 NIST Cybersecurity Framework v1.1 DE.CM-7 NIST Cybersecurity Framework v1.1 PR.AC-2 NIST SP 800-53 R4 PE-3e[HML]{2} NY DOH SSP v3.1 PE-3.IS1[HM]-1 OCR Audit Protocol (2016) 164.310(a)(2)(iv)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to HIPAA Security Rule Subject to HITRUST De-ID Framework Requirements Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance
Level 2 Implementation:	Level 1 plus: Security perimeters, such as any boundaries where security controls are in place to protect assets from unauthorized access, are clearly defined, and the siting and strength of each of the perimeters depend on the security requirements of the assets within the perimeter (public, sensitive, and restricted areas). A manned reception area or other means to control physical access to the site or building is in place. Access to sites and buildings is restricted to authorized personnel only (sensitive and restricted areas). Different levels of scrutiny are applied to public areas in which non-employees are expected, such as: offices, hallways, and communications closet, data center. All fire doors on a security perimeter are alarmed, monitored, and tested in conjunction with the walls to establish the required level of resistance in accordance with suitable regional, national, and international standards. They operate in accordance with local fire code in a fail-safe manner.
Level 2 Control Standard Mapping:	45 CFR Part § 164.310(c) HIPAA.SR-3 AICPA 2017 CC6.4 CMSRs v3.1 SC-24 (HIGH; MOD) COBIT 5 DSS05.05 CSA CCM v3.0.1 DCS-02 De-ID Framework v1 Public Access to Sensitive Areas: General FFIEC IS v2016 A.6.8 FFIEC IS v2016 A.8.1(e)

	ISO/IEC 27002:2013 11.1.1 ISO/IEC 27799:2016 11.1.1 NIST Cybersecurity Framework v1.1 DE.CM-2 NIST Cybersecurity Framework v1.1 DE.CM-7 NIST Cybersecurity Framework v1.1 DE.DP-2 NIST Cybersecurity Framework v1.1 PR.AC-2 NRS 603A.215.1 NY DOH SSP v3.1 MP-4.IS.CSP2[HM]-0 NY DOH SSP v3.1 PE-3.IS1[HM]-2 NY DOH SSP v3.1 PE-3.IS3[HM]-0 NY DOH SSP v3.1 PE-3a2[M]-0 PCI DSS v3.2.1 9.1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to Banking Requirements Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: Information assets and facilities managed by the organization are physically separated from those managed by third-parties. Two barriers to access covered information under normal security are required: 1. secured perimeter/locked container; 2. locked perimeter/secured interior; or 3. locked perimeter/security container. Covered information is containerized in areas where none, other than authorized employees, may have access afterhours.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 PE-03 (HIGH; MOD) CSA CCM v3.0.1 DCS-02 FedRAMP PE-3 IRS Pub 1075 v2016 4.2 IRS Pub 1075 v2016 4.3 IRS Pub 1075 v2016 4.5 IRS Pub 1075 v2016 9.3.11.3 ISO/IEC 27002:2013 11.1.1 ISO/IEC 27799:2016 11.1.1 MARS-E v2 PE-3 NIST Cybersecurity Framework v1.1 PR.AC-2 NY DOH SSP v3.1 PE-3.IS.PII2[HM]-1 NY DOH SSP v3.1 PE-3.IS.PII2[HM]-2

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation:	Minimum protection standards require two physical barriers between FTI, and any individual not authorized to access FTI. The perimeter is enclosed by slab-to-slab walls constructed of durable materials and supplemented by periodic inspection. Any lesser-type partition must be supplemented by electronic intrusion detection and fire detection systems. All doors entering the space must be locked in accordance with Locking Systems for Secured Areas. In the case of a fence/gate, the fence must have intrusion detection devices or be continually guarded, and the gate must be either guarded or locked with intrusion alarms. A security room is a room that has been constructed to resist forced entry. The entire room must be enclosed by slab-to-slab walls constructed of approved materials (e.g., masonry brick, concrete) and supplemented by periodic inspection, and entrance must be limited to specifically authorized personnel. Door hinge pins must be non-removable or installed on the inside of the room. FTI must be containerized in areas where no persons, other than authorized employees or authorized contractors, may have access afterhours. A security guard, custodial services worker or landlord may have access to a locked building or a locked room if FTI is in a locked container. If FTI is in a locked room, but not in a locked container, the guard, janitor or landlord may have a key to the building but not to the room. During business hours, if authorized personnel serve as the second barrier between FTI and unauthorized individuals, the authorized personnel must wear an identification badge or credential clearly displayed, preferably worn above the waist.

Control Reference: 08.b Physical Entry Controls

Control Specification:	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Authentication; Authorization; Documentation and Records; Monitoring; Physical and Facility Security; Third-parties and Contractors; User Access

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 1 Subject to CMMC Level 2 Subject to HIPAA Security Rule Subject to NIST 800-171 Basic Level Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline

	Subject to Supplemental Requirements Subject to Texas Health and Safety Code
Level 1 Implementation:	At a minimum, the organization: 1. develops, approves and maintains a list of individuals with authorized access to the facility where the information system resides; 2. issues authorization credentials for facility access; 3. reviews the access list and authorization credentials periodically but no less than quarterly; and 4. removes individuals from the facility access list when access is no longer required. For facilities where the information system resides, the organization enforces physical access authorizations at defined entry/exit points to the facility where the information system resides, maintains physical access audit logs, and provides security safeguards the organization determines are necessary for areas officially designated as publicly accessible. Except those areas officially designated as publicly accessible, the organization maintains visitor access logs for facilities where information systems reside for at least three months and reviews visitor records periodically but no less than monthly. Visitor records contain: 1. name and organization of the person visiting; 2. signature of the visitor; 3. form of identification; 4. date of access; 5. time of entry and departure; 6. purpose of visit; and 7. name and organization of person visited. Access to areas where sensitive information (e.g., covered information, payment card data) is processed or stored is controlled and restricted to authorized persons only. All visitors are escorted and supervised (their activities monitored) unless their access has been previously approved. Third-party support service personnel are granted restricted access to secure areas or covered information processing facilities only when required. This access is authorized and monitored.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(d) 45 CFR Part § 164.310(a)(1) HIPAA.SR-0 45 CFR Part § 164.310(a)(2)(ii) HIPAA.SR-0 45 CFR Part § 164.310(a)(2)(iii) HIPAA.SR-2 45 CFR Part § 164.310(a)(2)(iv) HIPAA.SR-0 45 CFR Part § 164.310(c) HIPAA.SR-1 AICPA 2017 CC6.1 AICPA 2017 CC6.2 AICPA 2017 CC6.3 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMMC v1.0 PE.1.131-0 CMMC v1.0 PE.1.132-0 CMMC v1.0 PE.1.133-0 CMMC v1.0 PE.2.135-1 CMSRs v3.1 MA-02 (HIGH; MOD) CMSRs v3.1 PE-02 (HIGH; MOD) CMSRs v3.1 PE-03 (HIGH; MOD) CMSRs v3.1 PE-08 (HIGH; MOD) COBIT 5 DSS05.05 CSA CCM v3.0.1 DCS-07

	CSA CCM v3.0.1 DCS-09 De-ID Framework v1 Visitor Access: Policy FedRAMP MA-2 FedRAMP PE-2 FedRAMP PE-3 FFIEC IS v2016 A.6.8 FFIEC IS v2016 A.8.1(e) IRS Pub 1075 v2016 4.2 IRS Pub 1075 v2016 4.3.1 IRS Pub 1075 v2016 9.3.11.2 IRS Pub 1075 v2016 9.3.11.3 IRS Pub 1075 v2016 9.3.11.7 ISO/IEC 27002:2013 11.1.2 ISO/IEC 27799:2016 11.1.2 MARS-E v2 MA-2 MARS-E v2 PE-2 MARS-E v2 PE-3 MARS-E v2 PE-7 MARS-E v2 PE-7(1) MARS-E v2 PE-8 NIST 800-171 r2 3.10.1-0 NIST 800-171 r2 3.10.2-1 NIST 800-171 r2 3.10.3-0 NIST 800-171 r2 3.10.4-0 NIST Cybersecurity Framework v1.1 DE.CM-2 NIST Cybersecurity Framework v1.1 DE.CM-7 NIST Cybersecurity Framework v1.1 DE.DP-2 NIST Cybersecurity Framework v1.1 PR.AC-2 NIST SP 800-53 R4 PE-2[HML]{0} NIST SP 800-53 R4 PE-3a[HML]{1} NIST SP 800-53 R4 PE-3b[HML]{0} NIST SP 800-53 R4 PE-3c[HML]{0} NRS 603A.215.1 NY DOH SSP v3.1 PE-2.IS.CSP1[HML]-0 NY DOH SSP v3.1 PE-2a[M]-0 NY DOH SSP v3.1 PE-2b[M]-0 NY DOH SSP v3.1 PE-2c[M]-0 NY DOH SSP v3.1 PE-2d[M]-0 NY DOH SSP v3.1 PE-3.IS.PII1[HM]-0 NY DOH SSP v3.1 PE-3.IS2[HM]-0 NY DOH SSP v3.1 PE-3a[M]-0 NY DOH SSP v3.1 PE-3b[M]-0 NY DOH SSP v3.1 PE-3c[M]-0 NY DOH SSP v3.1 PE-6b[M]-2 PCI DSS v3.2.1 9.4 PCI DSS v3.2.1 9.4.1 SR v6.4 8a-0 SR v6.4 8b-0 SR v6.4 9.2-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to CMMC Level 3 Subject to HIPAA Security Rule Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High)

	Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to Supplemental Requirements
Level 2 Implementation:	Level 1 plus: A visitor log is required including: 1. the date and time of entry and departure; 2. the visitor's name; 3. the organization represented; and 4. the employee authorizing physical access. The log is reviewed no less than monthly and upon occurrence of organization-defined security events and retained for at least two years in accordance with the organization's retention policy. Visitors are only granted access for specific and authorized purposes and are issued with instructions on the security requirements of the area and on emergency procedures. Authentication controls (e.g., access control card plus PIN) are used to authorize and validate all access. Access must be authorized and based on individual job function. An audit trail of all access is securely maintained. The organization ensures onsite personnel and visitors can be easily distinguished. All employees, contractors, third-party users and all visitors are required to wear some form of visible identification and immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification. Visitors are given a badge or access device that identifies them as non-employees, and they are required to surrender the badge or device before leaving the facility or upon expiration. The organization ensures onsite personnel and visitor identification (e.g., badges) are revoked or terminated when expired or when access is no longer authorized, and all physical access mechanisms, such as keys, access cards and combinations, are returned disabled or changed. Identification is also updated when access requirements change to ensure their status can be easily distinguished. Access rights to secure areas are regularly reviewed, at a minimum every 90 days, and updated or revoked when necessary. A restricted area, security room, or locked room is used to control access to areas containing covered and/or confidential information. These areas will be controlled accordingly.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(d) 45 CFR Part § 164.310(a)(2)(iii) HIPAA.SR-3 AICPA 2017 CC6.4 CMMC v1.0 MP.3.124-2 CMSRs v3.1 PE-03 (HIGH; MOD) CMSRs v3.1 PE-06 (HIGH; MOD) CMSRs v3.1 PE-08 (HIGH; MOD) COBIT 5 DSS05.05 De-ID Framework v1 Physical Access: Identification Policy De-ID Framework v1 Physical Access: Inappropriate Use De-ID Framework v1 Physical Security: General FedRAMP PE-3 FedRAMP PE-8 FFIEC IS v2016 A.6.8 FFIEC IS v2016 A.8.1(e) IRS Pub 1075 v2016 4.3.2 IRS Pub 1075 v2016 9.3.11.3 IRS Pub 1075 v2016 9.3.11.6 ISO/IEC 27002:2013 11.1.2

	ISO/IEC 27799:2016 11.1.2 MARS-E v2 PE-3 MARS-E v2 PE-6 MARS-E v2 PE-8 NIST 800-171 r2 3.8.5-2 NIST Cybersecurity Framework v1.1 DE.CM-2 NIST Cybersecurity Framework v1.1 DE.CM-7 NIST Cybersecurity Framework v1.1 DE.DP-2 NIST Cybersecurity Framework v1.1 PR.AC-2 NIST Cybersecurity Framework v1.1 PR.PT-1 NIST Cybersecurity Framework v1.1 RS.CO-3 NIST SP 800-53 R4 PE-3e[HML]{1} NIST SP 800-53 R4 PE-6b[HML]{1} NIST SP 800-53 R4 PE-8[HML]{0} NRS 603A.215.1 NY DOH SSP v3.1 PE-3e[M]-0 NY DOH SSP v3.1 PE-3g[M]-0 NY DOH SSP v3.1 PE-6.IS.CSP1[HML]-0 NY DOH SSP v3.1 PE-6b[M]-1 NY DOH SSP v3.1 PE-8a[M]-0 NY DOH SSP v3.1 PE-8b[M]-0 PCI DSS v3.2.1 9.1 PCI DSS v3.2.1 9.2 PCI DSS v3.2.1 9.3 PCI DSS v3.2.1 9.4 PCI DSS v3.2.1 9.4.2 PCI DSS v3.2.1 9.4.3 PCI DSS v3.2.1 9.4.4 SR v6.4 9.1-0 TJC IM.02.01.03, EP 5

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to Banking Requirements Subject to CMMC Level 1 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to HITRUST De-ID Framework Requirements Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: Doors to internal secure areas lock automatically, implement a door delay alarm, and are equipped with electronic locks (e.g., keypad, card swipe).

	The organization inventories physical access devices within every 90 days. Combinations and keys for organization-defined high-risk entry/exit points are changed within every 365 days and when keys are lost, or combinations are compromised. Intruder detection systems are installed to national, regional or international standards and regularly tested, at a minimum annually, to cover all external doors and accessible windows. Unoccupied areas are alarmed at all times. Cover is also provided for other areas (e.g., computer room or communications rooms), specifically, sensitive and restricted areas. The organization monitors and investigates notifications from physical intrusion alarms and surveillance equipment. Alarms are regularly tested to ensure proper operation. The organization maintains an electronic log of alarm system events and regularly reviews the logs no less than monthly.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(d) CMMC v1.0 PE.1.134-2 CMMC v1.0 PE.1.134-3 CMSRs v3.1 PE-03 (HIGH; MOD) CMSRs v3.1 PE-03(01) (HIGH) CMSRs v3.1 PE-06(01) (HIGH; MOD) De-ID Framework v1 Perimeter Security (Alarms): General De-ID Framework v1 Perimeter Security (Alarms): Logging FedRAMP PE-3 FedRAMP PE-6 FedRAMP PE-6(1) FFIEC IS v2016 A.6.8 IRS Pub 1075 v2016 4.3 IRS Pub 1075 v2016 4.3.2 IRS Pub 1075 v2016 4.3.3 IRS Pub 1075 v2016 9.3.11.3 IRS Pub 1075 v2016 9.3.11.6 ISO/IEC 27002:2013 11.1.1 ISO/IEC 27799:2016 11.1.1 MARS-E v2 PE-3 MARS-E v2 PE-6(1) NIST Cybersecurity Framework v1.1 DE.CM-2 NIST Cybersecurity Framework v1.1 DE.DP-2 NIST Cybersecurity Framework v1.1 DE.DP-3 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 PR.AC-2 NIST Cybersecurity Framework v1.1 RS.AN-1 NIST Cybersecurity Framework v1.1 RS.CO-3 NIST SP 800-53 R4 PE-3(3)[S]{0} NIST SP 800-53 R4 PE-3(6)[S]{0} NIST SP 800-53 R4 PE-3g[HML]{2} NIST SP 800-53 R4 PE-6(1)[HM]{0} NIST SP 800-53 R4 PE-6b[HML]{2} NY DOH SSP v3.1 PE-3.IS.CSP1[HML]-0 NY DOH SSP v3.1 PE-3f[M]-0 NY DOH SSP v3.1 PE-6(1)[M]-0 NY DOH SSP v3.1 PE-6a[M]-2

Level CMS Implementation Requirements

Level CMS Implementation:	The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at defined physical spaces (defined in the applicable security plan) containing a concentration of information system components (e.g., server rooms, media storage areas, data and communications centers, etc.).

	The organization employs automated mechanisms to facilitate the maintenance and review of access records.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	A visitor access log containing specific data elements will be used to authenticate and authorize visitor's access to any facility where FTI resides, either electronically or in paper, at the location where the outside (2nd) barrier is breached. The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at spaces where FTI is received, processed, stored, or transmitted. Unauthorized access to areas containing FTI during duty and non-duty hours must be denied. This can be done utilizing a combination of methods: secured or locked perimeter, secured area or containerization. The physical security and control of computers and electronic media must be addressed. Computer operations must be in a secure area with restricted access. A restricted area visitor log will be maintained at a designated entrance to the restricted area, and all visitors (persons not assigned to the area) entering the area are directed to the designated entrance. The entry control monitor verifies the identity of visitors by comparing the name and signature entered into the register with some type of photo identification card. Visitor access records include, for example, name/organization of the person visiting, signature of the visitor, form(s) of identification, date of access, time of entry and departure, purpose of visit, and name/organization of person visited. Whenever cleaning and maintenance personnel are working in restricted areas containing FTI, the cleaning and maintenance activities must be performed in the presence of an authorized employee.

Level HIX Implementation Requirements

Level HIX Implementation:	The organization authorizes physical access to the facility where the information system resides and information is received, processed, stored, or transmitted based on position or role.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	At a minimum, visitor access records must include the following information: (i) name and organization of the person visiting; (ii) visitor’s signature; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. The organization restricts unescorted access to the facility where the information system resides to personnel with (one or more): security clearances for all information contained within the system, formal access authorizations for all information contained within the system, need for access to all information contained within the system, and/or organization-defined credentials.

Level PCI Implementation Requirements

Level PCI Implementation:	The organization ensures visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained. Visitor logs include the name of the onsite personnel (workforce member) authorizing physical access.

Control Reference: 08.c Securing Offices, Rooms, and Facilities

Control Specification:	Physical security for offices, rooms, and facilities shall be designed and applied.
Factor Type:	Organizational
Topics:	Physical and Facility Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation:	Account is taken of relevant health and safety regulations and standards when securing facilities.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) ISO/IEC 27002:2013 11.1.3 ISO/IEC 27799:2016 11.1.3 NIST Cybersecurity Framework v1.1 DE.DP-2 NIST Cybersecurity Framework v1.1 ID.GV-3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to FedRAMP Certification Subject to HITRUST De-ID Framework Requirements Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)

Level 2 Implementation:	Level 1 plus: Critical facilities are sited to avoid access by the public. For particularly sensitive and restricted facilities (e.g., data centers and communication closets), buildings are unobtrusive and give minimum indication of their purpose, with no obvious signs outside or inside the building identifying the presence of information processing activities. Directories and internal telephone books identifying locations of covered information processing facilities are not readily accessible by the public. Video cameras or other access control mechanisms are implemented and secured to monitor individual physical access to sensitive areas. These devices are protected from tampering or disabling of the device. The results of the mechanisms are reviewed regularly and correlated with other entries and access control information (e.g., audit trails, sign-in sheets, authorization levels, maintenance logs). The information from cameras or other access control mechanisms is stored for at least three months in accordance with the organization's retention policy. Automated mechanisms are used to recognize potential intrusions and initiate designated response actions.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CIS CSC v7.1 12.7 CMSRs v3.1 PE-03 (HIGH; MOD) COBIT 5 DS5.7 COBIT 5 DSS05.05 CSA CCM v3.0.1 DCS-06 De-ID Framework v1 Public Access to Sensitive Areas: General De-ID Framework v1 Video Surveillance: General FedRAMP PE-3 FFIEC IS v2016 A.6.8 FFIEC IS v2016 A.8.1(e) IRS Pub 1075 v2016 9.3.11.3 ISO/IEC 27002:2013 11.1.3 ISO/IEC 27799:2016 11.1.3 MARS-E v2 PE-3 NIST Cybersecurity Framework v1.1 DE.CM-2 NIST Cybersecurity Framework v1.1 DE.CM-3 NIST Cybersecurity Framework v1.1 DE.CM-7 NIST Cybersecurity Framework v1.1 PR.AC-2 NIST SP 800-53 R4 PE-6(2)[S]{0} NIST SP 800-53 R4 PE-6(3)[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 PE-6a[M]-3 PCI DSS v3.2.1 9.1.1

Control Reference: 08.d Protecting Against External and Environmental Threats

Control Specification:	Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Awareness and Training; Physical and Facility Security; Third-parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	

Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Supplemental) Subject to Texas Health and Safety Code
Level 1 Implementation:	The organization develops, disseminates, and reviews/updates annually: 1. a formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. The following controls are implemented to avoid damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster: 1. appropriate fire extinguishers are located throughout the facility, and are no more than 50 feet away from critical electrical components; and 2. fire detectors (e.g., smoke or heat activated) are installed on and in the ceilings and floors.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) AICPA 2017 CC3.1 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 PE-01 (HIGH; MOD) CMSRs v3.1 PE-13 (HIGH; MOD) CSA CCM v3.0.1 BCR-05 FedRAMP PE-1 FFIEC IS v2016 A.6.8 IRS Pub 1075 v2016 9.3.11.1 ISO/IEC 27002:2013 11.1.4 ISO/IEC 27799:2016 11.1.4 MARS-E v2 PE-1 MARS-E v2 PE-13 NIST Cybersecurity Framework v1.1 PR.IP-5 NIST SP 800-53 R4 PE-13(4)[S]{0} PMI DSP Framework PR.DS-3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Supplemental) Subject to Texas Health and Safety Code
Level 2 Implementation:	Level 1 plus: Any security threats presented by neighboring premises are identified (e.g., a fire in a neighboring building, water leaking from the roof or in floors below ground level, or an explosion in the street).

	Fire prevention training is included in the regular training programs provided to the organization personnel. Appropriate fire suppression systems (e.g., sprinklers, gas) are implemented throughout the building and within secure areas containing information processing devices. For facilities not staffed continuously, these suppression systems are automated. The building's HVAC system is configured to automatically shut down upon fire detection.
Level 2 Control Standard Mapping:	CMSRs v3.1 PE-13 (HIGH; MOD) CMSRs v3.1 PE-13(03) (HIGH; MOD) CSA CCM v3.0.1 BCR-05 FedRAMP PE-13(3) FFIEC IS v2016 A.6.8 ISO/IEC 27002:2013 11.1.4 ISO/IEC 27002:2013 9.1.4 ISO/IEC 27799:2016 11.1.4 MARS-E v2 AT-3 MARS-E v2 PE-13 MARS-E v2 PE-13(3) NIST Cybersecurity Framework v1.1 PR.IP-5 NIST SP 800-53 R4 AT-3(1)[S]{0} NIST SP 800-53 R4 PE-13(3)[HM]{0} NY DOH SSP v3.1 PE-13[M]-1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to Banking Requirements Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: Water detectors are located in the dropped ceilings and raised floors to detect leaks or possible flooding. The organization protects the information systems from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel. Fire suppression and detection devices/systems that are supported by an independent energy source are implemented and maintained.

	Fire authorities are automatically notified when a fire alarm is activated.
Level 3 Control Standard Mapping:	CMSRs v3.1 PE-13 (HIGH; MOD) CMSRs v3.1 PE-13(01) (HIGH) CMSRs v3.1 PE-13(02) (HIGH) CMSRs v3.1 PE-15 (HIGH; MOD) CMSRs v3.1 PE-15(01) (HIGH) CSA CCM v3.0.1 BCR-05 FedRAMP PE-13 FedRAMP PE-13(2) FedRAMP PE-15 FFIEC IS v2016 A.6.8 ISO/IEC 27002:2013 11.1.4 ISO/IEC 27799:2016 11.1.4 MARS-E v2 PE-13 MARS-E v2 PE-13(1) MARS-E v2 PE-13(2) MARS-E v2 PE-15 NIST Cybersecurity Framework v1.1 PR.IP-5 NIST SP 800-53 R4 PE-13[HML]{0} NIST SP 800-53 R4 PE-15[HML]{0} NY DOH SSP v3.1 PE-13[M]-2 NY DOH SSP v3.1 PE-15[M]-0

Level CMS Implementation Requirements

Level CMS Implementation:	The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alert defined personnel or roles (defined in the applicable security plan). Fire suppression devices/systems activate automatically and automatically notify the organization and emergency responders in the event of a fire.

Level HIX Implementation Requirements

Level HIX Implementation:	The organization employs fire suppression devices/systems for the information system that activate automatically and notify the organization-specified personnel and emergency responders in the event of a fire.

Control Reference: 08.e Working in Secure Areas

Control Specification:	Physical protection and guidelines for working in secure areas shall be designed and applied.
Factor Type:	Organizational
Topics:	Personnel; Physical and Facility Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to IRS Pub 1075 Compliance

Level 1 Implementation:	The arrangements for working in secure areas include controls for the employees, contractors, and third-party users working in the secure area, as well as other third-party activities taking place there. Personnel are only aware of the existence of, or activities within, a secure area on a need-to-know basis. Unsupervised working in secure areas is avoided both for safety reasons and to prevent opportunities for malicious activities. Vacant secure areas are physically locked and periodically checked. Photographic, video, audio or other recording equipment such as cameras in mobile devices, are not allowed unless otherwise authorized.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) ISO/IEC 27002:2013 11.1.5 ISO/IEC 27799:2016 11.1.5 NIST Cybersecurity Framework v1.1 PR.AC-2 NIST Cybersecurity Framework v1.1 PR.IP-5

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	All computers, electronic media, and removable media containing FTI, must be kept in a secured area under the immediate protection and control of an authorized employee or locked up. When not in use, the media must be promptly returned to a proper storage area/container.

Control Reference: 08.f Public Access, Delivery, and Loading Areas

Control Specification:	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
Factor Type:	Organizational
Topics:	Media and Assets; Physical and Facility Security; User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	Access to a delivery and loading area from outside of the building is restricted to identified and authorized personnel. The delivery and loading area are designed so that supplies can be unloaded without delivery personnel gaining access to other parts of the building. The external doors of a delivery and loading area are secured when the internal doors are opened. Incoming material is registered in accordance with asset management procedures on entry to the site. Incoming and outgoing shipments are physically segregated, where possible.

Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 PE-16 (HIGH; MOD) CSA CCM v3.0.1 DCS-08 FedRAMP PE-16 IRS Pub 1075 v2016 4.3.1 IRS Pub 1075 v2016 9.3.11.8 ISO/IEC 27002:2013 11.1.6 ISO/IEC 27799:2016 11.1.6 MARS-E v2 PE-16 NIST Cybersecurity Framework v1.1 PR.AC-2 NIST Cybersecurity Framework v1.1 PR.IP-5 NY DOH SSP v3.1 PE-16[M]-2

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	
Level 2 Implementation:	Level 1 plus: Incoming material is inspected for potential threats before this material is moved from the delivery and loading area to the point of use.
Level 2 Control Standard Mapping:	CSA CCM v3.0.1 DCS-08 ISO/IEC 27002:2013 11.1.6 ISO/IEC 27799:2016 11.1.6 NIST Cybersecurity Framework v1.1 PR.IP-5

Objective Name: 08.02 Equipment Security

Control Objective:	To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

Control Reference: 08.g Equipment Siting and Protection

Control Specification:	Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
Factor Type:	Organizational
Topics:	Media and Assets; Physical and Facility Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations

Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to HITRUST De-ID Framework Requirements Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to Texas Health and Safety Code Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	Guidelines for eating, drinking, and smoking in proximity to information assets are established. Lightning protection is applied to all buildings, and lightning protection filters (e.g., surge protectors) are fitted to all incoming power and communications lines. Information assets handling covered and/or confidential information are positioned, and the viewing angle restricted to reduce the risk of information being viewed by unauthorized persons during their use. Storage devices are secured to avoid unauthorized access. Device locks are distributed and implemented for equipment containing covered and/or confidential information. Types of locks include, but are not limited to, slot locks, port controls, peripheral switch controls and cable traps. The organization restricts physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines. The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and, for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy. Controls are implemented to minimize the risk of potential physical threats including theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism. The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. The following controls are implemented to avoid damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster: 1. Hazardous or combustible materials are stored at a safe distance from a secure area; 2. bulk supplies such as stationery are not stored within a secure area; and 3. fallback equipment and back-up media are stored at a safe distance to avoid damage from disaster affecting the main site.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 A1.2 AICPA 2017 CC6.4 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 AC-18 (HIGH; MOD) CMSRs v3.1 PE-01 (HIGH; MOD) CMSRs v3.1 PE-18 (HIGH) CSA CCM v3.0.1 BCR-06 De-ID Framework v1 Physical and Environmental Security: General

	De-ID Framework v1 Physical Security: General FedRAMP AC-18 FedRAMP PE-1 HITRUST IRS Pub 1075 v2016 4.3 IRS Pub 1075 v2016 4.3.2 IRS Pub 1075 v2016 9.3.11.1 IRS Pub 1075 v2016 9.3.11.10 ISO/IEC 27002:2013 11.1.4 ISO/IEC 27002:2013 11.2.1 ISO/IEC 27799:2016 11.1.4 ISO/IEC 27799:2016 11.2.1 MARS-E v2 AC-18 MARS-E v2 PE-1 MARS-E v2 PE-18 NIST Cybersecurity Framework v1.1 PR.IP-5 NIST SP 800-53 R4 PE-18(1)[S]{0} NIST SP 800-53 R4 PE-18[H]{2} NIST SP 800-53 R4 PE-19(1)[S]{0} NIST SP 800-53 R4 PE-19[S]{2} NIST SP 800-53 R4 PE-9(2)[S]{2} NIST SP 800-53 R4 SC-28(2)[S]{0} NIST SP 800-53 R4 SC-40(1)[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 PE-18[HN]-1 PCI DSS v3.2.1 9.1.3 PCI DSS v3.2.1 9.9 PCI DSS v3.2.1 9.9.2

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to FedRAMP Certification Subject to IRS Pub 1075 Compliance Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline
Level 2 Implementation:	Level 1 plus: Equipment is sited to minimize unnecessary access into work areas. Environmental conditions, such as temperature and humidity, are monitored for conditions which could adversely affect the operation of information assets. Items requiring special protection are isolated to reduce the general level of protection required. The use of special protection methods, such as keyboard membranes, is implemented for equipment in industrial environments.
Level 2 Control Standard	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 A1.2

Mapping:	CMSRs v3.1 PE-14 (HIGH; MOD) CMSRs v3.1 PE-18 (HIGH) CSA CCM v3.0.1 BCR-06 FedRAMP PE-14 FedRAMP PE-14(2) IRS Pub 1075 v2016 4.3.2 IRS Pub 1075 v2016 9.3.11.10 IRS Pub 1075 v2016 9.4.4 IRS Pub 1075 v2016 9.4.9 ISO/IEC 27002:2013 11.2.1 ISO/IEC 27799:2016 11.2.1 MARS-E v2 PE-14 MARS-E v2 PE-18 NIST Cybersecurity Framework v1.1 PR.IP-5 NIST SP 800-53 R4 PE-14(1)[S]{0} NIST SP 800-53 R4 PE-14(2)[S]{0} NIST SP 800-53 R4 PE-18[H]{1} NY DOH SSP v3.1 PE-14b[M]-0 NY DOH SSP v3.1 PE-18[HN]-2

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The service provider measures temperature at server inlets and humidity levels by dew point.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	Multifunction Devices (MFDs) are locked with a mechanism to prevent physical access to the hard disk. Place fax machines in a secured area.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	When sending or receiving faxes containing PII: (i) fax machines must be located in a locked room with a trusted staff member having custodial coverage over outgoing and incoming transmissions, or fax machines must be located in a secured area; (ii) accurate broadcast lists and other preset numbers of frequent fax recipients must be maintained; and (iii) a cover sheet must be used that explicitly provides guidance to the recipient that includes a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information.

Level PCI Implementation Requirements

Level PCI Implementation:	The organization periodically inspects payment card device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).

Control Reference: 08.h Supporting Utilities

Control Specification:	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
Factor Type:	Organizational

Topics:	Contingency Planning; Maintenance; Monitoring; Physical and Facility Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline
Level 1 Implementation:	All supporting utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning are adequate for the systems they are supporting. Support utilities are regularly inspected and tested to ensure their proper functioning and to reduce any risk from their malfunction or failure. A suitable electrical supply is provided that conforms to the equipment manufacturer's specifications. An uninterruptable power supply (UPS) to support orderly closedown is required for equipment supporting critical business operations. Power contingency plans cover the action to be taken on failure of the UPS. UPS equipment and generators are regularly checked to ensure they have adequate capacity and are tested in accordance with the manufacturer's recommendations. The water supply is stable and adequate to supply air conditioning, humidification equipment and fire suppression systems, where used. Malfunctions in the water supply system may damage equipment or prevent fire suppression from acting effectively.
Level 1 Control Standard Mapping:	AICPA 2017 A1.2 CMSRs v3.1 PE-11(01) (HIGH) CSA CCM v3.0.1 BCR-03 CSA CCM v3.0.1 BCR-08 FedRAMP PE-11 ISO/IEC 27002:2013 11.2.2 ISO/IEC 27799:2016 11.2.2 MARS-E v2 PE-11 NIST Cybersecurity Framework v1.1 ID.BE-4 NIST Cybersecurity Framework v1.1 PR.IP-5 NIST SP 800-53 R4 PE-11[HM]{0} NY DOH SSP v3.1 PE-11[M]-1 NY DOH SSP v3.1 PE-15.IS1[HML]-1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to FedRAMP Certification Subject to FISMA Compliance

	Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The organization maintains temperature and humidity levels in facilities where critical information processing systems reside within acceptable vendor-recommended levels and monitors these levels at an organization-defined frequency. Organizations evaluate the level of alert and follow prescribed guidelines for that alert level, alert component management of possible loss of service and/or media, and, if necessary, report damage and provide remedial action. Implement contingency plan. Emergency lighting is provided in case of main power failure that covers emergency exists and evacuation routes within the facility. Emergency power-off switches are located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency. These devices are protected from accidental activation. A master power switch or emergency cut-off switch is implemented and maintained, prominently marked and protected by a cover, for data centers, servers, and mainframe rooms. An alarm system to detect malfunctions in the supporting utilities is evaluated and installed if required. Only authorized maintenance personnel are permitted to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.
Level 2 Control Standard Mapping:	CMSRs v3.1 PE-09 (HIGH; MOD) CMSRs v3.1 PE-10 (HIGH; MOD) CMSRs v3.1 PE-12 (HIGH; MOD) CMSRs v3.1 PE-14 (HIGH; MOD) FedRAMP PE-10 FedRAMP PE-12 FedRAMP PE-14 FedRAMP PE-14(2) FedRAMP PE-9 ISO/IEC 27002:2013 11.2.1 ISO/IEC 27002:2013 11.2.2 ISO/IEC 27002:2013 11.2.4 ISO/IEC 27799:2016 11.2.1 ISO/IEC 27799:2016 11.2.2 ISO/IEC 27799:2016 11.2.4 MARS-E v2 PE-10 MARS-E v2 PE-12 MARS-E v2 PE-14 MARS-E v2 PE-9 NIST Cybersecurity Framework v1.1 ID.BE-4 NIST Cybersecurity Framework v1.1 PR.AC-2 NIST Cybersecurity Framework v1.1 PR.IP-5 NIST SP 800-53 R4 PE-10a[HM]{0} NIST SP 800-53 R4 PE-10b[HM]{0} NIST SP 800-53 R4 PE-10c[HM]{0} NIST SP 800-53 R4 PE-12(1)[S]{0} NIST SP 800-53 R4 PE-12[HML]{0} NIST SP 800-53 R4 PE-14[HML]{0} NY DOH SSP v3.1 PE-10.IS1[HM]-0 NY DOH SSP v3.1 PE-10a[M]-0 NY DOH SSP v3.1 PE-10b[M]-0 NY DOH SSP v3.1 PE-10c[M]-0 NY DOH SSP v3.1 PE-12[M]-0

	NY DOH SSP v3.1 PE-14.IS1[HM]-0 NY DOH SSP v3.1 PE-14.IS1[L]-0 NY DOH SSP v3.1 PE-14.IS2[HM]-0 NY DOH SSP v3.1 PE-14.IS3[HM]-0 NY DOH SSP v3.1 PE-14a[M]-0

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	
Level 3 Implementation:	Level 2 plus: Voice services are adequate to meet local legal requirements for emergency communications.
Level 3 Control Standard Mapping:	CMSRs v3.1 CP-08 (HIGH; MOD) CSA CCM v3.0.1 BCR-03 ISO/IEC 27002:2013 11.2.2 ISO/IEC 27799:2016 11.2.2 MARS-E v2 CP-8 NIST Cybersecurity Framework v1.1 ID.BE-4 NIST Cybersecurity Framework v1.1 ID.GV-3

Level CMS Implementation Requirements

Level CMS Implementation:	The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Level HIPAA Implementation Requirements

Level HIPAA Implementation:	Level 1 Providers: A back-up generator is considered if processing is required to continue in case of a prolonged power failure. An adequate supply of fuel is available to ensure that the generator, if used, can perform for a prolonged period. Level 2 Providers: A back-up generator is implemented, and an adequate supply of fuel is available to ensure that the generator can perform for a prolonged period. Generators are regularly checked to ensure they have adequate capacity and are tested in accordance with the manufacturer's recommendations. Level 3 Providers: Multiple power sources or a separate power substation are used. Telecommunications equipment is connected to the utility provider by at least two diverse routes to prevent failure in one connection path removing voice services. The organization develops telecommunications service agreements that contain priority of service (Telecommunications Service Priority) provisions.

Level Providers Implementation Requirements	
Level Providers Implementation:	Level 1 Providers: A back-up generator is considered if processing is required to continue in case of a prolonged power failure. An adequate supply of fuel is available to ensure that the generator, if used, can perform for a prolonged period. Level 2 Providers: A back-up generator is implemented, and an adequate supply of fuel is available to ensure that the generator can perform for a prolonged period. Generators are regularly checked to ensure they have adequate capacity and are tested in accordance with the manufacturer's recommendations. Level 3 Providers: Multiple power sources or a separate power substation are used. Telecommunications equipment is connected to the utility provider by at least two diverse routes to prevent failure in one connection path removing voice services. The organization develops telecommunications service agreements that contain priority of service (Telecommunications Service Priority) provisions.

Control Reference: 08.i Cabling Security

Control Specification:	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.
Factor Type:	Organizational
Topics:	Media and Assets; Physical and Facility Security; Network Security

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline
Level 1 Implementation:	The organization protects power equipment and power cabling for the information system from damage and destruction. Access to patch panels and cable rooms is controlled. A documented patch list is used to reduce the possibility of errors. Clearly identifiable cable and equipment markings are used to minimize handling errors, such as accidental patching of wrong network cables.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) CMSRs v3.1 PE-09 (HIGH; MOD) CSA CCM v3.0.1 DCS-09 FedRAMP PE-9 ISO/IEC 27002:2013 11.2.3 ISO/IEC 27799:2016 11.2.3 MARS-E v2 PE-9 NIST Cybersecurity Framework v1.1 PR.AC-2 NIST Cybersecurity Framework v1.1 PR.IP-5 NIST SP 800-53 R4 PE-9(2)[S]{1} NIST SP 800-53 R4 PE-9[HM]{0} NY DOH SSP v3.1 PE-9[M]-0 TJC IM.02.01.03, EP 5

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to CMMC Level 2 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: Power and telecommunications lines into information processing facilities are underground, where possible, or subject to adequate alternative protection. Network cabling is protected from unauthorized interception or damage, for example, by using a conduit or by avoiding routes through public areas. Power cables are segregated from communications cables to prevent interference (only applicable where copper telecommunications cables are used). Armored conduit and locked rooms or boxes at inspection and termination points are installed. Alternative routings and/or transmission media providing appropriate security are used. Electromagnetic shielding is used to protect the cables. The organization controls physical access to information system distribution and transmission lines within organizational facilities by disabling any physical ports (e.g., wiring closets, patch panels, etc.) not in use. The organization implements physical and/or logical controls to restrict access to publicly accessible network jacks.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMMC v1.0 PE.2.135-2 CMSRs v3.1 PE-04 (HIGH; MOD) CSA CCM v3.0.1 BCR-03 FedRAMP PE-4 IRS Pub 1075 v2016 9.3.11.4 IRS Pub 1075 v2016 9.3.16.6 ISO/IEC 27002:2013 11.2.3 ISO/IEC 27799:2016 11.2.3 MARS-E v2 PE-4 NIST Cybersecurity Framework v1.1 PR.AC-2 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST SP 800-53 R4 PE-19[S]{1} NIST SP 800-53 R4 PE-3(1)[H]{0} NIST SP 800-53 R4 PE-3(5)[S]{1}

	NIST SP 800-53 R4 PE-3(5)[S]{2} NIST SP 800-53 R4 PE-4[HM]{0} NIST SP 800-53 R4 SC-37(1)[S]{1} NIST SP 800-53 R4 SC-37[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 PE-4.IS1[HM]-0 NY DOH SSP v3.1 PE-4[M]-0 PCI DSS v3.2.1 9.1.2

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	
Level 3 Implementation:	Level 2 plus: Technical sweeps and physical inspections are initiated for unauthorized devices being attached to the cables.
Level 3 Control Standard Mapping:	CMSRs v3.1 CM-08(03) (HIGH; MOD) ISO/IEC 27002:2013 11.2.3 ISO/IEC 27799:2016 11.2.3 NIST Cybersecurity Framework v1.1 PR.AC-2

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	If encryption is not used to protect the transmission of FTI, the agency must ensure that all network infrastructure, access points, wiring, conduits, and cabling are within the control of authorized agency personnel.

Control Reference: 08.j Equipment Maintenance

Control Specification:	Equipment shall be correctly maintained to ensure its continued availability and integrity. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Documentation and Records; Maintenance; Media and Assets

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	

Level 1 Regulatory Factors:	Subject to CMMC Level 2 Subject to NIST 800-171 Basic Level Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Texas Health and Safety Code
Level 1 Implementation:	The organization develops, disseminates, and reviews/updates annually: 1. a formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls. Equipment is maintained in accordance with the supplier's recommended service intervals and specifications. Only authorized maintenance personnel carry out repairs and service equipment. Appropriate controls are implemented when equipment is scheduled for maintenance (e.g., authorization levels) taking into account whether this maintenance is performed by personnel on site or external to the organization. The organization: 1. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; 2. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and 3. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations. The organization monitors and controls nonlocal maintenance and diagnostic activities; and prohibits nonlocal system maintenance unless explicitly authorized, in writing, by the CIO or his/her designated representative. If nonlocal maintenance and diagnostic actives are authorized, the organization: 1. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and as documented in the security plan for the information system; 2. Employs strong identification and authentication techniques in the establishment of nonlocal maintenance and diagnostic sessions; 3. Maintains records for nonlocal maintenance and diagnostic activities; and 4. Terminates all sessions and network connections when nonlocal maintenance is completed. The organization obtains maintenance support and/or spare parts for defined key information system components (defined in the applicable security plan) within the applicable Recovery Time Objective (RTO) specified in the contingency plan. All requirements imposed by insurance policies are complied with.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC3.1 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMMC v1.0 MA.2.111-0 CMMC v1.0 MA.2.112-2

	CMMC v1.0 MA.2.114-0 CMSRs v3.1 MA-01 (HIGH; MOD) CMSRs v3.1 MA-04 (HIGH; MOD) CMSRs v3.1 MA-04(01) (HIGH; MOD) CMSRs v3.1 MA-04(03) (HIGH) CMSRs v3.1 MA-05 (HIGH; MOD) CMSRs v3.1 MA-05(01) (HIGH) CMSRs v3.1 MA-06 (HIGH; MOD) CRR v2016 CCM:G2.Q10 CSA CCM v3.0.1 BCR-07 FedRAMP MA-1 FedRAMP MA-4 FedRAMP MA-5 FedRAMP MA-6 IRS Pub 1075 v2016 9.3.9.1 IRS Pub 1075 v2016 9.3.9.4 IRS Pub 1075 v2016 9.3.9.5 ISO/IEC 27002:2013 11.2.4 ISO/IEC 27799:2016 11.2.4 MARS-E v2 MA-1 MARS-E v2 MA-4 MARS-E v2 MA-4(1) MARS-E v2 MA-5 MARS-E v2 MA-6 NIST 800-171 r2 3.7.1-0 NIST 800-171 r2 3.7.2-2 NIST 800-171 r2 3.7.6-0 NIST Cybersecurity Framework v1.1 PR.MA-1 NIST Cybersecurity Framework v1.1 PR.MA-2 NIST SP 800-53 R4 MA-4(5)a[S]{0} NIST SP 800-53 R4 MA-4(5)b[S]{1} NIST SP 800-53 R4 MA-4a[HML]{0} NIST SP 800-53 R4 MA-5(2)[S]{1} NIST SP 800-53 R4 MA-5(4)[S]{2} NIST SP 800-53 R4 MA-5[HML]{0} NIST SP 800-53 R4 MA-6(1)[S]{0} NIST SP 800-53 R4 MA-6(2)[S]{0} NIST SP 800-53 R4 MA-6[HM]{0} NY DOH SSP v3.1 MA-4[M]-0 NY DOH SSP v3.1 MA-5a[M]-0 NY DOH SSP v3.1 MA-5b[M]-0 NY DOH SSP v3.1 MA-5c[M]-0 NY DOH SSP v3.1 MA-6[M]-0 NY DOH SSP v3.1 PE-12.IS1[HML]-1 NY DOH SSP v3.1 PE-13.IS1[HML]-1 NY DOH SSP v3.1 PE-14c[M]-1 NY DOH SSP v3.1 PE-15(1).IS1[H]-1 NY DOH SSP v3.1 PE-15.IS1[HML]-2 NY DOH SSP v3.1 PE-9.IS1[HM]-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to CMMC Level 3 Subject to NIST 800-171 Derived Level Subject to NY OHIP Moderate-Plus Security Baseline

Level 2 Implementation:	Level 1 plus: Covered and/or confidential information is cleared from the equipment, or the maintenance personnel are sufficiently cleared prior to all maintenance. Records are kept of all suspected or actual faults and all preventive and corrective maintenance including: 1. date and time of maintenance; 2. name of individual performing maintenance; 3. name of escort; 4. a description of maintenance performed; and 5. a list of equipment removed or replaced. The organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMMC v1.0 MA.3.115-0 CMSRs v3.1 MA-02 (HIGH; MOD) CMSRs v3.1 MA-02(02) (HIGH) CRR v2016 CCM:G2.Q11 CRR v2016 CCM:G2.Q9 CSA CCM v3.0.1 BCR-07 FedRAMP MA-2 IRS Pub 1075 v2016 9.3.9.2 ISO/IEC 27002:2013 11.2.4 ISO/IEC 27799:2016 11.2.4 MARS-E v2 MA-2 MARS-E v2 MA-2(1) NIST 800-171 r2 3.7.3-0 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.MA-1 NY DOH SSP v3.1 MA-4.IS2[HML]-1 NY DOH SSP v3.1 MA-4c[M]-0

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to CMMC Level 2 Subject to CMMC Level 3 Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Basic Level Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate)

	Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: The organization approves, controls and monitors the use of information system maintenance tools (e.g., hardware and software brought into the organization for diagnostic/repair actions). All maintenance tools carried into the facility by maintenance personnel are inspected for improper or unauthorized modifications. All media containing diagnostic and test programs is checked for malicious code prior to the media being used in the information system. The organization documents the requirements (e.g., policies and procedures) for the establishment and use of nonlocal maintenance and diagnostic connections in the security plan for the information system.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMMC v1.0 MA.2.112-1 CMMC v1.0 MA.3.116-0 CMSRs v3.1 MA-03 (HIGH; MOD) CMSRs v3.1 MA-03(01) (HIGH; MOD) CMSRs v3.1 MA-03(02) (HIGH; MOD) CMSRs v3.1 MA-04(02) (HIGH; MOD) CRR v2016 CCM:G2.Q10 CSA CCM v3.0.1 BCR-07 FedRAMP MA-3 FedRAMP MA-3(1) FedRAMP MA-3(2) FedRAMP MA-4(2) IRS Pub 1075 v2016 9.3.9.3 IRS Pub 1075 v2016 9.3.9.4 MARS-E v2 MA-3 MARS-E v2 MA-3(1) MARS-E v2 MA-3(2) MARS-E v2 MA-4(2) NIST 800-171 r2 3.7.2-1 NIST 800-171 r2 3.7.4-0 NIST Cybersecurity Framework v1.1 DE.CM-4 NIST Cybersecurity Framework v1.1 PR.MA-1 NIST SP 800-53 R4 MA-3(1)[HM]{0} NIST SP 800-53 R4 MA-3(2)[HM]{0} NIST SP 800-53 R4 MA-3[HM]{0} NIST SP 800-53 R4 MA-4(2)[HM]{0} NIST SP 800-53 R4 MA-4b[HML]{0} NY DOH SSP v3.1 MA-3(1)[M]-0 NY DOH SSP v3.1 MA-3(2)[M]-0 NY DOH SSP v3.1 MA-3[M]-0 NY DOH SSP v3.1 MA-4(2)[M]-0 NY DOH SSP v3.1 MA-4(3)a[HN]-1 NY DOH SSP v3.1 MA-4a[M]-0

Level CMS Implementation Requirements

Level CMS Implementation:	The organization: 1. Implements procedures, for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, which include the following requirements i. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; ii. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access

	approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and iii. Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system. If password-based authentication is used during remote maintenance, change the passwords following each remote maintenance service. The organization audits nonlocal maintenance and diagnostic sessions using available auditable events and reviews the records of the sessions. The organization: 1. requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or 2. removes the component to be serviced from the information system and, prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to sensitive information) before removal from organizational facilities, and after the service is performed, inspected, and sanitized the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the information system. Automated mechanisms are implemented to schedule, conduct, and document maintenance and repairs as required, producing up-to-date, accurate, complete and available records of all maintenance and repair actions, needed, in process, and completed. The equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within control of the organization, be destroyed, or an exemption is obtained from the CMS CIO or his/her designated representative explicitly authorizing removal of the equipment from the facility. The organization requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or removes the component to be serviced from the information system and, prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organization information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the information system.
Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation:	The equipment is appropriately sanitized before release. If the equipment cannot be sanitized, the equipment remains within control of the organization, is destroyed, or an exemption is obtained from the information owner explicitly authorizing removal of the equipment from the facility.
Level HIX Implementation Requirements	
Level HIX Implementation:	The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: 1. Verifying there is no organizational information contained in the equipment; 2. Sanitizing or destroying the equipment; 3. Retaining the equipment within the facility; or

	4. Obtaining a written exemption from the CIO or his/her designated representative explicitly authorizing removal of the equipment from the facility.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The organization (i) schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; (ii) approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on-site or removed to another location; (iii) requires that the applicable Business Owner (or an official designated in the applicable security plan) explicitly approves the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; (iv) sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; (v) checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and (vi) includes defined maintenance-related information (defined in the applicable security plan) in organizational maintenance records.

Control Reference: 08.k Security of Equipment Off-Premises

Control Specification:	Security shall be applied to off-site equipment taking into account the different risks of working outside the organization's premises.
Factor Type:	Organizational
Topics:	Authorization; IT Organization and Management Roles and Responsibilities; Media and Assets; Physical and Facility Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	Regardless of ownership, the use of any information processing equipment outside the organization's premises is authorized by management. This includes equipment used by remote workers, even where such use is permanent (e.g., a core feature of the employee's role, such as for ambulance personnel or therapists). Equipment and media taken off the premises are not left unattended in public places. Portable computers are carried as hand luggage and disguised where possible when travelling. Manufacturers' instructions for protecting equipment are observed at all times (e.g., protection against exposure to strong electromagnetic fields). Home-working controls are applied, including lockable filing cabinets, clear desk policy, and access controls for computers and secure communication with the office.

	Adequate insurance coverage is in place to protect equipment off-site. Security risks (e.g., of damage, theft, or eavesdropping) may vary considerably between locations and are taken into account in determining the most appropriate controls.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 AC-20 (HIGH; MOD) CMSRs v3.1 MP-05 (HIGH; MOD) CMSRs v3.1 PE-17 (HIGH; MOD) CSA CCM v3.0.1 DCS-04 CSA CCM v3.0.1 DCS-05 FedRAMP MP-5 FedRAMP PE-17 IRS Pub 1075 v2016 9.3.10.5 IRS Pub 1075 v2016 9.3.11.9 ISO/IEC 27002:2013 11.2.6 ISO/IEC 27002:2013 6.2 ISO/IEC 27002:2013 6.2.1 ISO/IEC 27002:2013 6.2.2 ISO/IEC 27799:2016 11.2.6 ISO/IEC 27799:2016 6.2 ISO/IEC 27799:2016 6.2.1 ISO/IEC 27799:2016 6.2.2 MARS-E v2 AC-20 MARS-E v2 MP-5 MARS-E v2 PE-17 NIST Cybersecurity Framework v1.1 PR.DS-3 NRS 603A.215.1 NY DOH SSP v3.1 PE-12.IS1[HML]-2 NY DOH SSP v3.1 PE-13.IS1[HML]-2 NY DOH SSP v3.1 PE-14c[M]-2 NY DOH SSP v3.1 PE-15(1).IS1[H]-2

Control Reference: 08.l Secure Disposal or Re-Use of Equipment

Control Specification:	All items of equipment containing storage media shall be checked to ensure that any covered information and licensed software has been removed or securely overwritten prior to disposal. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Data Loss Prevention; Media and Assets

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 1 Subject to FISMA Compliance Subject to HIPAA Security Rule Subject to HITRUST De-ID Framework Requirements Subject to IRS Pub 1075 Compliance Subject to Joint Commission Accreditation Subject to MARS-E Requirements Subject to NIST 800-171 Basic Level Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to Texas Health and Safety Code

	Subject to the CMS Minimum Security Requirements (High) Subject to the State of Nevada Security of Personal Information Requirements
Level 1 Implementation:	Surplus equipment is stored securely while not in use and disposed of or sanitized when no longer required. Devices containing covered and/or confidential information are physically destroyed, or the information is destroyed, deleted, or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function. The following are appropriate techniques to securely remove information: 1. disk wiping 2. degaussing The following are appropriate techniques to securely destroy electronic and hard copy media: 1. shredding disk platters 2. disintegration 3. grinding surfaces 4. incineration 5. pulverization 6. melting See NIST SP 800-88 Guidelines for Media Sanitization for more information on implementing media sanitization and destruction techniques. The organization renders information unusable, unreadable, or indecipherable on system media, both digital and non-digital, prior to disposal or release for reuse using organization-defined sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies. The organization destroys media containing sensitive information that cannot be sanitized.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.310(d)(2)(i) HIPAA.SR-2 45 CFR Part § 164.310(d)(2)(ii) HIPAA.SR-0 AICPA 2017 CC6.5 CMMC v1.0 MP.1.118-0 CMSRs v3.1 DM-02 (HIGH; MOD) CMSRs v3.1 MP-06 (HIGH; MOD) COBIT 5 DS1.4 COBIT 5 DS11.4 COBIT 5 DS11.6 COBIT 5 DSS05.03 COBIT 5 DSS05.06 CRR v2016 AM:G6.Q6 CSA CCM v3.0.1 DSI-07 De-ID Framework v1 Disposal: Data Destruction Procedures FedRAMP MP-6 FFIEC IS v2016 A.6.16(e) FFIEC IS v2016 A.6.18(e) IRS Pub 1075 v2016 8.2 IRS Pub 1075 v2016 8.3 IRS Pub 1075 v2016 9.3.10.6 ISO/IEC 27002:2013 11.2.7 ISO/IEC 27799:2016 11.2.7 MARS-E v2 DM-2 MARS-E v2 MP-6 NIST 800-171 r2 3.8.3-0 NIST Cybersecurity Framework v1.1 PR.DS-3 NIST Cybersecurity Framework v1.1 PR.IP-6 NIST SP 800-53 R4 MP-8[S]{4} NRS 603A.200.1

	NRS 603A.200.2.b.1 NRS 603A.200.2.b.2 NY DOH SSP v3.1 MA-4(3)b[HN]-2 NY DOH SSP v3.1 MP-6.PII1[M]-1 NY DOH SSP v3.1 MP-6a[M]-1 OCR Guidance for Unsecured PHI (2)(i) OCR Guidance for Unsecured PHI (2)(ii) PCI DSS v3.2.1 9.8.1 PCI DSS v3.2.1 9.8.2 TJC IM.02.01.03, EP 7

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	For CSPs, the hypervisor enforces sanitization of the instance (container) image file space upon release. The organization securely stores surplus equipment while not in use, disposed of, or sanitized in accordance with NIST 800-88 when no longer required. CSPs support the capability to sanitize disk space when released from an instance (container) image file and sanitization is in accordance with NIST SP 800-88, as amended.

Control Reference: 08.m Removal of Property

Control Specification:	Equipment, information or software shall not be taken off site without prior authorization.
Factor Type:	Organizational
Topics:	Authorization; Documentation and Records; Media and Assets; Personnel; Third-parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to Joint Commission Accreditation Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	Equipment, information or software are not to be taken off site without prior authorization. Employees, contractors and third-party users who have authority to permit off-site removal of assets are clearly identified. Time limits for equipment removal are set and returns checked for compliance. Where necessary and appropriate, equipment is recorded as being removed off site and recorded when returned.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 PE-16 (HIGH; MOD) CSA CCM v3.0.1 DCS-04

FedRAMP PE-16
IRS Pub 1075 v2016 4.3.1
IRS Pub 1075 v2016 9.3.11.8
ISO/IEC 27002:2013 11.2.5
ISO/IEC 27799:2016 11.2.5
MARS-E v2 PE-16
NIST Cybersecurity Framework v1.1 PR.DS-3
NIST Cybersecurity Framework v1.1 PR.IP-6
NIST SP 800-53 R4 PE-16[HML]{1}
NIST SP 800-53 R4 PE-16[HML]{2}
NY DOH SSP v3.1 PE-16[M]-1
TJC IM.02.01.03, EP 4

Control Category: 09.0 - Communications and Operations Management

Objective Name: 09.01 Documented Operating Procedures

Control Objective:	To ensure that operating procedures are documented, maintained and made available to all users who need them.

Control Reference: 09.a Documented Operations Procedures

Control Specification:	Operating procedures shall be documented, maintained, and made available to all users who need them.
Factor Type:	System
Topics:	Cryptography; Documentation and Records; Policies and Procedures

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (Supplemental) Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	Documented procedures are prepared for system activities associated with information and communication assets, including computer start-up and close-down procedures, backup of data, equipment maintenance, media handling, electronic communications, computer room, and mail handling management, and safety. The operating procedures specify the detailed instructions for the execution of each job including: 1. processing and handling of information; 2. the backup of data; 3. scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times; 4. instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities; 5. support contacts in the event of unexpected operational or technical difficulties; 6. special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output from failed jobs; 7. system restart and recovery in the event of system failure; and 8. the management of audit-trail and system log information. Operating procedures, and the documented procedures for system activities, are treated as formal documents and changes authorized by management.

Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(k) CMSRs v3.1 AC-01 (HIGH; MOD) CMSRs v3.1 AT-01 (HIGH; MOD) CMSRs v3.1 AU-01 (HIGH; MOD) CMSRs v3.1 CA-01 (HIGH; MOD) CMSRs v3.1 CM-01 (HIGH; MOD) CMSRs v3.1 CP-01 (HIGH; MOD) CMSRs v3.1 IA-01 (HIGH; MOD) CMSRs v3.1 IR-01 (HIGH; MOD) CMSRs v3.1 PE-01 (HIGH; MOD) CMSRs v3.1 PL-01 (HIGH; MOD) CMSRs v3.1 PM-01 (HIGH; MOD) CMSRs v3.1 PS-01 (HIGH; MOD) CMSRs v3.1 RA-01 (HIGH; MOD) CMSRs v3.1 SA-01 (HIGH; MOD) CMSRs v3.1 SC-01 (HIGH; MOD) CMSRs v3.1 SI-01 (HIGH; MOD) CSA CCM v3.0.1 BCR-04 CSA CCM v3.0.1 BCR-10 FedRAMP AT-1 FedRAMP AU-1 FedRAMP CA-1 FedRAMP CM-1 FedRAMP CP-1 FedRAMP IA-1 FedRAMP IR-1 FedRAMP MA-1 FedRAMP MP-1 FedRAMP PE-1 FedRAMP PL-1 FedRAMP PS-1 FedRAMP RA-1 FedRAMP SA-1 FedRAMP SC-1 FedRAMP SI-1 FFIEC IS v2016 A.6.1 IRS Pub 1075 v2016 9.3.1.1 IRS Pub 1075 v2016 9.3.10.1 IRS Pub 1075 v2016 9.3.11.1 IRS Pub 1075 v2016 9.3.12.1 IRS Pub 1075 v2016 9.3.13.1 IRS Pub 1075 v2016 9.3.14.1 IRS Pub 1075 v2016 9.3.15.1 IRS Pub 1075 v2016 9.3.16.1 IRS Pub 1075 v2016 9.3.17.1 IRS Pub 1075 v2016 9.3.2.1 IRS Pub 1075 v2016 9.3.3.1 IRS Pub 1075 v2016 9.3.4.1 IRS Pub 1075 v2016 9.3.5.1 IRS Pub 1075 v2016 9.3.6.1 IRS Pub 1075 v2016 9.3.7.1 IRS Pub 1075 v2016 9.3.8.1 IRS Pub 1075 v2016 9.3.9.1 IRS Pub 1075 v2016 Exhibit 10 ISO/IEC 27002:2013 12.1.1 ISO/IEC 27799:2016 12.1.1 MARS-E v2 AC-1 MARS-E v2 AT-1 MARS-E v2 AU-1 MARS-E v2 CA-1 MARS-E v2 CM-1 MARS-E v2 CP-1 MARS-E v2 IA-1 MARS-E v2 IR-1 MARS-E v2 MA-1 MARS-E v2 MP-1 MARS-E v2 PE-1 MARS-E v2 PL-1 MARS-E v2 PM-1 MARS-E v2 PS-1 MARS-E v2 RA-1 MARS-E v2 SA-1 MARS-E v2 SC-1

	MARS-E v2 SI-1 NIST SP 800-53 R4 AU-15[S]{0} NIST SP 800-53 R4 SI-7(16)[S]{0} NRS 603A.215.1 PCI DSS v3.2.1 1.5 PCI DSS v3.2.1 10.9 PCI DSS v3.2.1 11.6 PCI DSS v3.2.1 2.5 PCI DSS v3.2.1 3.7 PCI DSS v3.2.1 4.3 PCI DSS v3.2.1 5.4 PCI DSS v3.2.1 6.7 PCI DSS v3.2.1 7.3 PCI DSS v3.2.1 8.8 PCI DSS v3.2.1 9.10

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	If data warehousing documentation is integrated with other security documents, these documents have a section dedicated to the data warehouse(s) to define controls specific to that environment. The organization ensures these documents: 1. describe how 'legacy system data' will be brought into the data warehouse and how the legacy data that is FTI will be cleansed for the extraction, transformation and loading (ETL) process; and 2. any unique issues related to data warehousing.

Level PCI Implementation Requirements

Level PCI Implementation:	The organization ensures operational procedures are documented, communicated (known to all parties) and in use for the following: 1. managing firewalls, 2. managing vendor defaults and other security parameters, 3. protecting stored cardholder data, 4. encrypting transmissions of cardholder data, 5. protecting systems against malware, 6. developing and maintaining secure systems and applications, 7. restricting access to cardholder data, 8. identification and authentication, 9. restricting physical access to cardholder data, 10. monitoring access to network resources and cardholder data, and 11. security monitoring and testing.

Control Reference: 09.b Change Management

Control Specification:	Changes to information assets and systems shall be controlled and archived. *Required for HITRUST Certification CSF v9.6
Factor Type:	System
Topics:	IT Organization and Management Roles and Responsibilities; Media and Assets

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems

Level 1 Regulatory Factors:	Subject to Supplemental Requirements
Level 1 Implementation:	Changes to information assets, including systems, networks and network services, are controlled and archived.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 CM-03 (HIGH; MOD) CRR v2016 AM:G4.Q1 CRR v2016 CCM:G1.Q1 CRR v2016 CCM:G2.Q2 CRR v2016 CCM:MIL2.Q1 CRR v2016 CCM:MIL2.Q2 FedRAMP CM-3 FFIEC IS v2016 A.6.11 IRS Pub 1075 v2016 9.3.5.3 ISO/IEC 27002:2013 12.1.2 ISO/IEC 27799:2016 12.1.2 MARS-E v2 CM-3 NIST Cybersecurity Framework v1.1 PR.IP-3 SR v6.4 27-1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (Supplemental) Subject to Supplemental Requirements Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: Changes are managed strictly and consistently. Formal management responsibilities and procedures are in place to ensure satisfactory control of all changes to equipment, software or procedures, including: 1. the identification and recording of significant changes; 2. the planning and testing of changes; 3. the assessment of the potential impacts, including security impacts, of such changes; 4. the formal approval for proposed changes; and 5. the communication of change details to all relevant persons. Fallback procedures are defined and implemented, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 CM-03 (HIGH; MOD) CMSRs v3.1 CM-04 (HIGH; MOD) CMSRs v3.1 CM-05 (HIGH; MOD) CRR v2016 CCM:G1.Q1 CRR v2016 CCM:G1.Q5 CRR v2016 CCM:G2.Q2

	CRR v2016 CCM:G2.Q3 CRR v2016 CCM:MIL2.Q1 CRR v2016 CCM:MIL2.Q2 CRR v2016 CCM:MIL2.Q4 FedRAMP CM-3 FedRAMP CM-4 FedRAMP CM-5 FFIEC IS v2016 A.6.11 IRS Pub 1075 v2016 9.3.5.3 IRS Pub 1075 v2016 9.3.5.4 IRS Pub 1075 v2016 9.3.5.5 ISO/IEC 27001:2013 8.1 ISO/IEC 27002:2013 12.1.2 ISO/IEC 27799:2016 12.1.2 MARS-E v2 CM-3 MARS-E v2 CM-4 MARS-E v2 CM-5 NIST Cybersecurity Framework v1.1 PR.IP-3 NIST SP 800-53 R4 CM-5(6)[S]{2} SR v6.4 27-2 SR v6.4 7b.4-0

Level DGF Implementation Requirements

Level DGF Implementation:	Data Governance tools and technologies are tested and approved for interoperability.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The organization maintains a baseline configuration for information system development and test environments that is managed separately from the operational baseline configuration. The organization retains records of configuration-controlled changes to the information system for a minimum of three [3) years after the change. The organization ensures that all cryptographic mechanisms used to provide protection to sensitive information are under configuration management. The organization ensures changes in information system security functions are verified to be implemented per approved design. The system's security functions must be continuously monitored and evaluated to ensure they are operating as intended and changes do not have an adverse effect on system performance. Actions must be taken to verify that the provisioned security function implementation being assessed and/or monitored meets security function requirements and is an approved system configuration. The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Records reflecting all such changes must be generated, reviewed, and retained. Information system changes must be verified to meet system mission and user requirements. The following CMS hierarchy for implementing security configuration guidelines is used when an HHS-specific minimum security configuration does not exist, and to resolve configuration conflicts among multiple security guidelines: (i) USGCB; (ii) NIST NCP; Tier IV, then Tier III, Tier II, and Tier I, in descending order; (iii) Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG); (iv) National Security Agency (NSA) STIGs; (v) If formal government-authored checklists do not exist, then organizations are encouraged to use vendor or industry group (such as The Center

	for Internet Security [CIS]) checklists; (vi) In situations where no guidance exists, coordinate with CMS for guidance. CMS must collaborate within CMS and the HHS Cybersecurity Program, and other organizations through the HHS Continuous Monitoring and Risk Scoring (CMRS) working group to: (a) Establish baseline configurations and communicate industry and vendor best practices; and (b) Ensure deployed configurations are supported for security updates. (vii) All deviations from existing USGCB, NCP, DISA and/or NSA configurations must be documented.

Control Reference: 09.c Segregation of Duties

Control Specification:	Separation of duties shall be enforced to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Authorization; IT Organization and Management Roles and Responsibilities; Monitoring

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 3 Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (Supplemental) Subject to Supplemental Requirements
Level 1 Implementation:	Small organizations may find segregation of duties difficult to achieve, but the principle is applied as far as is possible and practicable. Whenever it is difficult to segregate controls, such as monitoring of activities, audit trails, management supervision, or a system of dual control (e.g., two individuals with separate responsibilities needing to work together to accomplish a task) are required. Security audit activities always remain independent.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) AICPA 2017 CC5.1 AICPA 2017 CC6.3 CMMC v1.0 AC.3.017-0 CRR v2016 AM:G5.Q6 FFIEC IS v2016 A.6.8(d) ISO/IEC 27002:2013 6.1.2 ISO/IEC 27799:2016 6.1.2 NIST 800-171 r2 3.1.4-0 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST SP 800-53 R4 CM-9(1)[S]{0} SR v6.4 7b.2-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions

	Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to FISMA Compliance Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline
Level 2 Implementation:	Level 1 plus: Segregation of duties is a method for reducing the risk of accidental or deliberate system misuse. No single person is able to access, modify or use assets without authorization or detection. The initiation of an event is separated from its authorization to reduce the possibility of collusion. The organization identifies duties that require separation and define information system access authorizations to support separation of duties. Job descriptions reflect accurately the assigned duties and responsibilities that support separation of duties. Incompatible duties are segregated across multiple users to minimize the opportunity for misuse or fraud. In cases where conflicting duties must be assigned to a single user, activity logging and log reviews by an independent party are required.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC1.3 AICPA 2017 CC3.3 CMSRs v3.1 AC-05 (HIGH; MOD) COBIT 5 DS05.04 COBIT 5 DS5.5 COBIT 5 DS5.7 FedRAMP AC-5 FFIEC IS v2016 A.6.8(d) IRS Pub 1075 v2016 9.3.1.5 ISO/IEC 27002:2013 6.1.2 ISO/IEC 27799:2016 6.1.2 MARS-E v2 AC-5 NIST Cybersecurity Framework v1.1 DE.CM-3 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST SP 800-53 R4 AC-3(2)[S]{2} NIST SP 800-53 R4 AC-5[HM]{0} NIST SP 800-53 R4 SA-11(3)a[S]{1} NIST SP 800-53 R4 SC-3(4)[S]{0} NY DOH SSP v3.1 AC-5a[M]-1 NY DOH SSP v3.1 AC-5c[M]-0

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3	

System Factors:	
Level 3 Regulatory Factors:	Subject to Banking Requirements Subject to FedRAMP Certification Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: The organization: 1. ensures that audit functions are not performed by security personnel responsible for administering access control; 2. maintains a limited group of administrators with access based upon the users' roles and responsibilities; 3. ensures that mission critical functions and information system support functions are divided among separate individuals; 4. ensures that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups; 5. ensures that an independent entity, not the Business Owner, System Developer(s)/Maintainer(s), or System Administrator(s) responsible for the information system, conducts information security testing of the information system; and 6. ensures that quality assurance and code reviews of custom-developed applications, scripts, libraries, and extensions are conducted by an independent entity, not the code developers.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 AC-05 (HIGH; MOD) COBIT 5 DS5.7 COBIT 5 DSS05.05 CSA CCM v3.0.1 IAM-05 FedRAMP AC-5 FFIEC IS v2016 A.6.8(d) IRS Pub 1075 v2016 9.3.1.5 ISO/IEC 27002:2013 6.1.2 ISO/IEC 27799:2016 6.1.2 MARS-E v2 AC-5 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST SP 800-53 R4 AC-2i[HML]{2} NIST SP 800-53 R4 AC-4(17)[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 AC-5.IS1[M]-0 NY DOH SSP v3.1 AC-5.IS3[M]-0 NY DOH SSP v3.1 AC-5.IS4[M]-0 PCI DSS v3.2.1 6.4.2

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	To use an Integrated Voice Response (IVR) system that provides FTI over the telephone to a customer, the agency must ensure independent security testing is conducted on the IVR system prior to implementation.

Control Reference: 09.d Separation of Development, Test, and Operational Environments

Control Specification:	Development, test, and operational environments shall be separated and controlled to reduce the risks of unauthorized access or changes to the operational system.
Factor Type:	System
Topics:	IT Organization and Management Roles and Responsibilities; Policies and Procedures

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	
Level 1 Implementation:	The organization minimizes any testing on production systems. When testing must be performed, a test plan is developed that documents all changes to the system and the procedures for undoing any changes made to the system (e.g., removing test accounts).
Level 1 Control Standard Mapping:	CRR v2016 CCM:G2.Q7 CSA CCM v3.0.1 IVS-08 ISO/IEC 27002:2013 12.1.2 ISO/IEC 27002:2013 12.1.4 ISO/IEC 27799:2016 12.1.2 ISO/IEC 27799:2016 12.1.4 NIST Cybersecurity Framework v1.1 PR.DS-7 NIST Cybersecurity Framework v1.1 PR.IP-3 NRS 603A.215.1 PCI DSS v3.2.1 6.4.1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The level of separation between operational, test, and development environments is identified, and controls are implemented to prevent operational issues, including: 1. along with removing accounts, a review of all custom code preceding the release to production or to customers must be completed in order to identify any possible coding vulnerability, to include at least the following: i. code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices;

	ii. code reviews ensure code is developed according to secure coding guidelines, iii. appropriate corrections are implemented prior to release, and iv. code-review results are reviewed and approved by management prior to release; 2. test data and accounts are removed completely before the application is placed into a production state; 3. organizations remove all custom application accounts, user IDs, and passwords before applications go from development to production or are released to customers; 4. rules for the transfer of software from development to operational status are defined and documented; 5. development and operational software run on different systems or computer processors and in different domains or directories; 6. compilers, editors, and other development tools or system utilities are not accessible from operational systems when not required; 7. the test system environment emulates the operational system environment as closely as possible; 8. users use different user profiles for operational and test systems, and menus display appropriate identification messages to reduce the risk of error; and 9. covered information is not copied into the test system environment.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CIS CSC v7.1 18.9 CMSRs v3.1 CM-02 (HIGH; MOD) CRR v2016 CCM:G1.Q1 CSA CCM v3.0.1 IVS-08 FedRAMP CM-2 IRS Pub 1075 v2016 9.3.5.2 IRS Pub 1075 v2016 Exhibit 10 ISO/IEC 27002:2013 12.1.4 ISO/IEC 27799:2016 12.1.4 MARS-E v2 CM-2 NIST Cybersecurity Framework v1.1 PR.DS-7 NRS 603A.215.1 PCI DSS v3.2.1 6.3.1 PCI DSS v3.2.1 6.3.2 PCI DSS v3.2.1 6.4.1 PCI DSS v3.2.1 6.4.3 PCI DSS v3.2.1 6.4.4

Level CMS Implementation Requirements

Level CMS Implementation:	All systems supporting development and pre-production testing are connected to an isolated network separated from production systems. Network traffic into and out of the development and pre-production testing environment is only permitted to facilitate system testing and is restricted by source and destination access control lists (ACLs) as well as ports and protocols.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	Whenever FTI is located on both production and test environments, these environments are to be segregated, especially in the development stages of the data warehouse.

Level HIX Implementation Requirements

Level HIX Implementation:	All systems supporting development and pre-production testing are connected to an isolated network separate from production systems. Network traffic into and out of the development and pre-production testing environment is only permitted to facilitate

	system testing and is restricted by source and destination access control lists as well as ports and protocols.

Level Supplemental Requirements	Implementation Requirements
Level Supplemental Requirements Implementation:	Separation between production and non-production (development, test/quality assurance) environments is established and controls are implemented to prevent operational issues.

Objective Name: 09.02 Control Third Party Service Delivery

Control Objective:	To ensure that third party service providers maintain security requirements and levels of service as part of their service delivery agreements.

Control Reference: 09.e Service Delivery

Control Specification:	It shall be ensured that the security controls, service definitions, and delivery levels included in the third-party service delivery agreement are implemented, operated and maintained by the third party. *Required for HITRUST Certification CSF v9.6
Factor Type:	System
Topics:	Monitoring; Requirements (Legal and Contractual); Services and Acquisitions; Third-parties and Contractors

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to HITRUST De-ID Framework Requirements Subject to Texas Health and Safety Code
Level 1 Implementation:	In an agreed service arrangement, service delivery by a third-party (e.g., a certification authority for the provision of cryptographic services) includes: 1. service definitions; 2. delivery levels; 3. security controls, including third-party personnel security, information classification, transmission, and authorization; 4. aspects of service management, including monitoring, auditing, impacts to the organizations resilience, and change management; and 5. issues of liability, reliability of services, and response times for the provision of services.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 201 CMR 17.03(2)(f)(2) CMSRs v3.1 SA-09 (HIGH; MOD) CRR v2016 EDM:G4.Q1 CSA CCM v3.0.1 STA-09 EU GDPR Article 32(4) FFIEC IS v2016 A.6.31(c)

	FFIEC IS v2016 A.6.31(g) ISO/IEC 27002:2013 15.1.1 ISO/IEC 27799:2016 15.1.1 NIST Cybersecurity Framework v1.1 DE.CM-6 NIST Cybersecurity Framework v1.1 PR.AT-3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to FTC Red Flags Rule Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to Supplemental Requirements Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The organization develops, disseminates, and reviews/updates annually a list of current service providers, which includes a description of the services provided. In the case of outsourcing arrangements, the organization plans the necessary transitions (of information, information processing systems, and anything else that needs to be moved), and ensures that security is maintained throughout the transition period. The service provider protects the company's data with reasonable controls (e.g., policies and procedures) designed to detect, prevent, and mitigate risk. The organization defines and documents oversight (e.g., governmental, organizational) and user roles and responsibilities with regard to external information system services. The organization ensures that the third-party maintains sufficient service capabilities together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster. The organization restricts the location of facilities that process, transmit or store covered information (e.g., to those located in the United States), as needed, based on its legal, regulatory, contractual and other security and privacy-related obligations.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 16 CFR Part § 681 Appendix A VI(c) 16 CFR Part § 681.1 (e)(4) AICPA 2017 CC9.2 CMSRs v3.1 SA-09 (HIGH; MOD) CRR v2016 EDM:G4.Q2 FedRAMP SA-9 FedRAMP SA-9(5) FFIEC IS v2016 A.6.31(a) FFIEC IS v2016 A.6.31(g) IRS Pub 1075 v2016 9.3.15.7 ISO/IEC 27001:2013 8.1 ISO/IEC 27002:2013 15.2.1 ISO/IEC 27799:2016 15.2.1 MARS-E v2 SA-9 NIST Cybersecurity Framework v1.1 DE.AE-4

	NIST Cybersecurity Framework v1.1 DE.CM-6 NIST Cybersecurity Framework v1.1 ID.AM-4 NIST Cybersecurity Framework v1.1 PR.AT-3 NIST Cybersecurity Framework v1.1 PR.DS-3 NIST SP 800-53 R4 SA-9(5)[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 SA-9(5).CSP[MN]-0 NY DOH SSP v3.1 SA-9(5).PII[MN]-2 PCI DSS v3.2.1 12.8 PCI DSS v3.2.1 12.8.1 PCI DSS v3.2.1 2.6 SR v6.4 45a-2
Level Community Supplemental Reqs 02	**Implementation Requirements**
Level Community Supplemental Reqs 02 Implementation:	The organization executes a master service agreement with a third-party service provider experienced in incident response and forensics on a contingency basis. The organization ensures that service contracts for incident management require the service provider to deliver immediate remote support and be on-site (if possible and/or where practical) within 48 hours of an incident.
Level De-ID Data Environment	**Implementation Requirements**
Level De-ID Data Environment Implementation:	If required in the applicable jurisdiction, health information including de-identified data is not accessed from off-shore; nor is such data received, stored, processed or disposed via information technology systems located off-shore. Otherwise, the entity must justify the off-shore disclosure.
Level FTI Custodians	**Implementation Requirements**
Level FTI Custodians Implementation:	The organization restricts the location of information systems that receive, process, store, or transmit FTI to areas within the United States territories, embassies, or military installations. FTI may not be accessed by agency employees, agents, representatives or contractors located outside of the United States or its territories, i.e., off-shore.
Level HIX	**Implementation Requirements**
Level HIX Implementation:	The outsourcing of information system services outside the continental U.S. must be authorized by the CIO of CMS, and the service contract or agreement must include language requiring the provider to be subject to U.S. Federal laws and regulations protecting personally identifiable information. Depending on the outcome of the risk assessment, the organization may need to restrict the location of information systems that receive, process, store, or transmit PII to areas within United States territories, embassies, or military installations. The organization: 1. Notifies CMS of plans to outsource information system services prior to the awarding of a contract; 2. Requires that providers of external information system services comply with organizational security requirements (consistent with 45 CFR 155.260(b)), define security and privacy roles and responsibilities in the service contract or agreement, and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

	3. Defines and documents oversight and user roles and responsibilities with regard to external information system services; 4. Ensures that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance; 5. Employs defined process, methods, and techniques (defined in the applicable security plan) to monitor security and privacy control compliance by external service providers on an ongoing basis; and 6. Notifies CMS at least 45 days prior to transmitting data into an external information service environment.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The organization defines and documents government oversight and user roles and responsibilities with regard to external information system services.

Control Reference: 09.f Monitoring and Review of Third-Party Services

Control Specification:	The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly to govern and maintain compliance with the service delivery agreements. *Required for HITRUST Certification CSF v9.6
Factor Type:	System
Topics:	Audit and Accountability; Documentation and Records; Incident Response; Requirements (Legal and Contractual); Services and Acquisitions; Third-parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	
Level 1 Implementation:	A periodic review of service level agreements (SLAs) is conducted at least annually and compared against the monitoring records.
Level 1 Control Standard Mapping:	16 CFR Part § 681 Appendix A VI(c) 16 CFR Part § 681.1 (e)(4) CRR v2016 EDM:G4.Q1 CRR v2016 EDM:G4.Q2 CRR v2016 EDM:MIL2.Q1 CSA CCM v3.0.1 STA-09 ISO/IEC 27002:2013 15.2.1 ISO/IEC 27799:2016 15.2.1 NIST Cybersecurity Framework v1.1 DE.CM-6 NIST Cybersecurity Framework v1.1 PR.AT-3 NRS 603A.215.1 PCI DSS v3.2.1 12.8 PCI DSS v3.2.1 12.8.4

Level 2 Implementation Requirements

Level 2	

Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to FTC Red Flags Rule Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The organization monitors security control compliance by external service providers on an ongoing basis. Monitoring involves a service management relationship and process between the organization and the third-party. Service performance levels are monitored to check adherence to the agreements. Service reports produced by the third-party are reviewed and regular progress meetings arranged as required by the agreements. third-party audit trails and records of security events, operational problems, failures, tracing of faults and disruptions related to the service delivered are reviewed. Information about information security incidents is provided to the incident response team. This information is reviewed by the third-party that experienced the incident and the organization which the third-party provides services to, as required by the agreements and any supporting guidelines and procedures. Any identified problems are resolved and reviewed by the organization as noted above. The organization monitors the network service features and service levels to detect abnormalities and violations. The organization periodically audits the network services to ensure that network service providers implement the required security features and meet the requirements agreed with management, including with new and existing regulations.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(3) 1 TAC § 390.2(a)(4)(A)(xi) 16 CFR Part § 681 Appendix A VI(c) 16 CFR Part § 681.1 (e) 16 CFR Part § 681.1 (e)(4) CMSRs v3.1 SA-09 (HIGH; MOD) CRR v2016 EDM:G4.Q2 CRR v2016 EDM:G4.Q3 CRR v2016 EDM:G4.Q4 CSA CCM v3.0.1 STA-09 FedRAMP SA-9 FFIEC IS v2016 A.6.21(b) IRS Pub 1075 v2016 9.3.15.7 ISO/IEC 27001:2013 8.1 ISO/IEC 27002:2013 13.1.2 ISO/IEC 27002:2013 15.2.1 ISO/IEC 27799:2016 13.1.2 ISO/IEC 27799:2016 15.2.1 MARS-E v2 SA-9 NIST Cybersecurity Framework v1.1 DE.CM-6 NIST Cybersecurity Framework v1.1 PR.AT-3 NIST Cybersecurity Framework v1.1 RS.CO-4 NIST Cybersecurity Framework v1.1 RS.MI-2 NIST SP 800-53 R4 IR-7(2)a[S]{1} NRS 603A.215.1 NY DOH SSP v3.1 SA-9c[M]-0

	PCI DSS v3.2.1 12.8 PCI DSS v3.2.1 12.8.4 PCI DSS v3.2.1 2.6

Level 3 Implementation Requirements	
Level 3 Organizational Factors:	
Level 3 System Factors:	
Level 3 Regulatory Factors:	
Level 3 Implementation:	Level 2 plus: The organization maintains sufficient overall control and visibility into all security aspects for covered and critical information or information processing systems accessed, processed or managed by a third-party. The organization ensures they retain visibility into security activities such as change management, identification of vulnerabilities, and information security incident reporting and response through a clearly defined reporting process, format and structure.
Level 3 Control Standard Mapping:	

Level CMS Implementation Requirements	
Level CMS Implementation:	The organization employs defined processes, methods and techniques (defined in the applicable security plan) to monitor security control compliance by external service providers on an ongoing basis.

Level Supplemental Requirements	Implementation Requirements
Level Supplemental Requirements Implementation:	Supplier (i) ensures all supplier entities performing any in-scope work are contractually obligated to comply with the organization's security requirements, or requirements that are no less stringent; (ii) ensure the use of the organization's information resources and in-scope information by supplier entities will only be for the performance of in-scope work; (iii) maintain and adhere to a documented program by which supplier entity compliance to the organization's security requirements is evaluated by supplier and all corrective actions are documented and implemented; and (iv) upon the organization’s request, supplier will provide documentation and/or evidence to adequately substantiate such compliance.

Control Reference: 09.g Managing Changes to Third Party Services

Control Specification:	Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.
Factor Type:	System
Topics:	Risk Management and Assessments; Services and Acquisitions; Third-parties and Contractors

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	
Level 1 Implementation:	The organization ensures that third-party organizations use appropriate change management procedures for any changes to a third-party service or organizational system (see 9.a and 10.k).
Level 1 Control Standard Mapping:	ISO/IEC 27001:2013 8.1 ISO/IEC 27002:2013 15.2.2 ISO/IEC 27799:2016 15.2.2 NIST Cybersecurity Framework v1.1 ID.BE-1 NIST Cybersecurity Framework v1.1 PR.AT-3

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	Subject to FTC Red Flags Rule
Level 2 Implementation:	Level 1 plus: Change management on a third-party service includes: 1. the assessment and explicit recording of the potential impacts, including security impacts, of such changes; 2. evaluating and implementing changes made by the organization for: i. enhancements to the current services offered, ii. development of any new applications and systems, iii. modifications or updates of the organization's policies and procedures, and iv. new controls to resolve information security incidents and to improve security; 3. evaluating and implementing changes in third-party services for: i. changes and enhancement to networks, ii. use of new technologies, iii. adoption of new products or newer versions/releases, iv. new development tools and environments, v. changes to physical location of service facilities, and vi. change of vendors.
Level 2 Control Standard Mapping:	16 CFR Part § 681 Appendix A VI(c) 16 CFR Part § 681.1 (e)(4) ISO/IEC 27001:2013 8.1 ISO/IEC 27002:2013 15.2.2 ISO/IEC 27799:2016 15.2.2 NIST Cybersecurity Framework v1.1 ID.BE-1 NIST Cybersecurity Framework v1.1 ID.RA-4

Objective Name: 09.03 System Planning and Acceptance

Control Objective:	To ensure that systems meet the businesses current and projected needs to minimize failures.

Control Reference: 09.h Capacity Management

Control Specification:	The availability of adequate capacity and resources shall be planned, prepared, and managed to deliver the required system performance. Projections of future capacity requirements shall be made to mitigate the risk of system overload.
Factor Type:	System
Topics:	IT Organization and Management Roles and Responsibilities; Monitoring; Planning

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Supplemental)
Level 1 Implementation:	The use of information and information system resources is monitored, and projections made of future capacity requirements to ensure adequate systems performance. Organizations allocate sufficient storage capacity to reduce the likelihood of exceeding capacity and reduce the impact on network infrastructure, e.g., bandwidth.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 AU-04 (HIGH; MOD) CRR v2016 CCM:G1.Q3 CSA CCM v3.0.1 IVS-04 FedRAMP AU-4 FFIEC IS v2016 A.8.1(p) IRS Pub 1075 v2016 9.3.3.5 ISO/IEC 27002:2013 12.1.3 ISO/IEC 27799:2016 12.1.3 MARS-E v2 AU-4 NIST Cybersecurity Framework v1.1 PR.DS-4 NIST SP 800-53 R4 SA-12(13)[S]{1}

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High) Subject to the EU GDPR

Level 2 Implementation:	Level 1 plus: Capacity and monitoring procedures include: 1. the identification of capacity requirements for each new and ongoing system/service; 2. the projection of future capacity requirements, taking into account current use, audit record storage requirements, projected trends, and anticipated changes in business requirements; and 3. the system monitoring and tuning to ensure and improve the availability and effectiveness of current systems. The information system takes the following additional actions in response to an audit storage capacity issue: 1. shutdown the information system; 2. stop generating audit records; or 3. overwrite the oldest records, in the case that storage media is unavailable. The organization protects against, or limits the effects of the types of denial of, service attacks defined in NIST SP 800-63 Rev. 1, Computer Security Incident Handling Guide, and the following websites: 1. SANS Organization www.sans.org/dosstep; 2. SANS Organization's Roadmap to Defeating DDoS www.sans.org/dosstep/roadmap.php; and 3. NIST CVE List National Vulnerability Database: http://nvd.nist.gov/home.cfm.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 A1.1 AICPA 2017 CC7.2 CIS CSC v7.1 6.4 CMSRs v3.1 AU-05 (HIGH; MOD) CMSRs v3.1 SC-05 (HIGH; MOD) CRR v2016 CCM:G1.Q3 CSA CCM v3.0.1 IVS-04 FedRAMP AU-5 FedRAMP SC-5 IRS Pub 1075 v2016 9.3.16.4 ISO/IEC 27002:2013 12.1.3 ISO/IEC 27799:2016 12.1.3 MARS-E v2 AU-5 MARS-E v2 SC-5 NIST Cybersecurity Framework v1.1 ID.BE-1 NIST Cybersecurity Framework v1.1 PR.DS-4 NIST Cybersecurity Framework v1.1 PR.PT-1 NY DOH SSP v3.1 AU-4.IS1[M]-0 NY DOH SSP v3.1 AU-4[M]-0 NY DOH SSP v3.1 SC-5[M]-0 NY DOH SSP v3.1 SC-5a[M]-0 NY DOH SSP v3.1 SC-5b[M]-0 NY DOH SSP v3.1 SC-5c[M]-0

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The information system protects the availability of resources by allocating resources by priority or quota protection safeguards.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	The agency must allocate audit record storage capacity to retain audit records for the required audit retention period of seven years.

Level Supplemental Requirements	**Implementation Requirements**
Level Supplemental Requirements Implementation:	The organization protects against or limits the effects of various types of denial-of-service attacks, including distributed denial-of-service attacks.

Control Reference: 09.i System Acceptance

Control Specification:	Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance to maintain security.
Factor Type:	System
Topics:	Awareness and Training; Documentation and Records; IT Organization and Management Roles and Responsibilities

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to NY OHIP Moderate-Plus Security Baseline
Level 1 Implementation:	Managers ensure that the requirements and criteria for acceptance of new systems are clearly defined, agreed, documented, and tested. New information systems, upgrades, and new versions are only migrated into production after obtaining formal acceptance from management.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 CM-03 (HIGH; MOD) CSA CCM v3.0.1 CCC-01 CSA CCM v3.0.1 CCC-05 FedRAMP CM-3 FedRAMP SA-4 IRS Pub 1075 v2016 9.3.15.4 IRS Pub 1075 v2016 9.3.5.3 ISO/IEC 27002:2013 14.2.2 ISO/IEC 27002:2013 14.2.9 ISO/IEC 27799:2016 14.2.2 ISO/IEC 27799:2016 14.2.9 MARS-E v2 CM-3 MARS-E v2 SA-4 NIST Cybersecurity Framework v1.1 PR.IP-2 NY DOH SSP v3.1 PM-10.IS.PHI1[M]-1 NY DOH SSP v3.1 PM-10.PII[M]-1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500

Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Supplemental Requirements Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The organization requires the developer of the information system, system component, or information system service to: 1. Create and implement a security assessment plan; 2. Perform unit, integration, system and regression testing/evaluation in accordance with organization-defined requirements for depth and coverage; 3. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; 4. Implement a verifiable flaw remediation process; and 5. Correct flaws identified during security testing/evaluation. The following actions are carried out prior to formal acceptance being provided: 1. an agreed set of security controls are in place; 2. consultation with affected persons, or representatives of affected groups, at all phases of the process; 3. preparation and testing of routine operating procedures to defined standards; 4. effective manual procedures; 5. evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times, such as month end; 6. evidence that an analysis has been carried out on the effect the new system has on the overall security of the organization; 7. training in the operation or use of new systems; 8. error recovery and restart procedures, and contingency plans; 9. ease of use (as this affects user performance and avoids human error); and 10. training in the new operation(s). Organizations ensure that the IT systems employed contain application functionality that enforces the approval of processes by different role holders. The impact of the installation of any new system is thoroughly analyzed and tested with the coverage of the extreme operational conditions of the current systems.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC6.1 CMSRs v3.1 CM-07 (HIGH; MOD) CMSRs v3.1 SA-11 (HIGH; MOD) CRR v2016 CCM:G2.Q7 CSA CCM v3.0.1 CCC-03 FedRAMP CM-7 FedRAMP SA-11 FFIEC IS v2016 A.6.28(a) FFIEC IS v2016 A.6.28(b) IRS Pub 1075 v2016 9.3.15.9 IRS Pub 1075 v2016 9.3.5.7 ISO/IEC 27002:2013 14.2.9 ISO/IEC 27799:2016 14.2.9 MARS-E v2 CM-7

	MARS-E v2 SA-11 NIST Cybersecurity Framework v1.1 PR.IP-2 NIST SP 800-53 R4 SA-11(7)[S]{0} NIST SP 800-53 R4 SA-11[HM]{0} NIST SP 800-53 R4 SA-15(1)[S]{1} NIST SP 800-53 R4 SA-4(3)[S]{0} NIST SP 800-53 R4 SA-4(5)a[S]{2} NIST SP 800-53 R4 SI-2b[HML]{0} NY DOH SSP v3.1 CA-2c[M]-0 NY DOH SSP v3.1 RA-5d[M]-2 NY DOH SSP v3.1 SA-11a[M]-0 NY DOH SSP v3.1 SA-11b[M]-0 NY DOH SSP v3.1 SA-11c[M]-0 NY DOH SSP v3.1 SA-11d[M]-0 NY DOH SSP v3.1 SA-11e[M]-0 SR v6.4 29a.1-1 SR v6.4 30-0

Level CMS Implementation Requirements

Level CMS Implementation:	The organization requires the developer of the information system, system component, or information system service to: 1. Create and implement a security assessment plan in accordance with, but not limited to, current CMS procedures; 2. Perform unit; integration; system; regression testing/evaluation in accordance with the CMS eXpedited Life Cycle (XLC); 3. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; 4. Implement a verifiable flaw remediation process; and 5. Correct flaws identified during security testing/evaluation. If the security control assessment results are used in support of the security authorization process for the information system, the organization ensures that no security relevant modifications of the information systems have been made subsequent to the assessment and after selective verification of the results. The organization uses hypothetical data when executing test scripts or in a test environment that is configured to comply with the security controls as if it is a production environment.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	The agency must submit a request to the IRS Office of Safeguards for authority to use live data for testing, providing a detailed explanation of the safeguards in place to protect the FTI over the Internet to a customer. To use a VoIP network that provides FTI to a customer, the agency must ensure security testing is conducted on the VoIP system prior to implementation with FTI.

Level HIX Implementation Requirements

Level HIX Implementation:	If the security control assessment results are used in support of the security authorization process for the information system, the organization ensures that no security relevant modifications of the information systems have been made subsequent to the assessment and after selective verification of the results. The organization uses hypothetical data when executing test scripts or in a test environment that is configured to comply with the security controls as if it is a production environment.

Objective Name: 09.04 Protection Against Malicious and Mobile Code

Control Objective:	Ensure that integrity of information and software is protected from malicious or unauthorized code.

Control Reference: 09.j Controls Against Malicious Code

Control Specification:	Detection, prevention, and recovery controls shall be implemented to protect against malicious code, and appropriate user awareness procedures on malicious code shall be provided. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Awareness and Training; Contingency Planning; Policies and Procedures; Viruses and Malware

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to HITRUST De-ID Framework Requirements Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to State of Massachusetts Data Protection Act Subject to Texas Health and Safety Code
Level 1 Implementation:	Protection against malicious code is based on malicious code detection and repair software, security awareness, and appropriate system access and change management controls. Formal policies are required, and technologies implemented for the timely installation and upgrade of the protective measures, including the installation and regular, automatic updating of anti-virus or anti-spyware software, including virus definitions, whenever updates are available. Periodic reviews/scans are required of installed software and the data content of systems to identify and, where possible, remove any unauthorized software. However, server environments for which the server software developer specifically recommends not installing host-based anti-virus and anti-spyware software, may address the requirement via a network-based malware detection (NBMD) solution. If an NBMD solution is used, the organization also: 1. disables USB ports; 2. prohibits the use of writable media (e.g., DVD-R); 3. restricts the use of read-only media (e.g., DVD-ROM) to legitimate commercial sources for legitimate business reasons (e.g., Linux installation disks); and 4. allows only whitelisted software to run on the system. The NBMD solution must be installed in-band, whether or not blocking is enabled. Cloud-based implementations with blocking enabled is preferred. If the organization chooses to implement a local solution and/or disables blocking, the decision must be supported by a formal risk analysis, and any additional risk formally accepted by management as required by its risk management policy.

	The organization employs anti-malware software that offers a centralized infrastructure that compiles information on file reputations or has administrators manually push updates to all machines. After applying an update, automated systems verify that each system has received its signature update. Procedures are defined for response to identification of malicious code or unauthorized software. Checking anti-virus or anti-spy software generates audit logs of checks performed. The checks carried out by the malicious code detection and repair software to scan computers and media include: 1. checking any files on electronic or optical media, and files received over networks, for malicious code before use; 2. checking electronic mail attachments and downloads for malicious code or file types that are unnecessary for the organization's business before use; this check is carried out at different places (e.g., at electronic mail servers, desk top computers and when entering the network of the organization); and 3. checking web traffic, such as HTML, JavaScript, and HTTP, for malicious code; and 4. checking removable media (e.g., USB tokens and hard drives, CDs/DVDs, FireWire devices, and external serial advanced technology attachment devices) when inserted. Formal policies are required prohibiting the use or installation of unauthorized software, including a prohibition of obtaining data and software from external networks. User awareness and training on these policies and methods are provided for all users on a regular basis. Bring your own device (BYOD) users are required to use anti-malware software (where supported).
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 201 CMR 17.04(7) AICPA 2017 CC6.8 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CIS CSC v7.1 7.8 CIS CSC v7.1 7.9 CIS CSC v7.1 8.1 CIS CSC v7.1 8.4 CMSRs v3.1 CM-11 (HIGH; MOD) CMSRs v3.1 SI-03 (HIGH; MOD) COBIT 5 DS5.9 COBIT 5 DSS05.01 CRR v2016 VM:G1.Q3 CSA CCM v3.0.1 MOS-17 CSA CCM v3.0.1 TVM-01 De-ID Framework v1 Anti-malware: General FedRAMP CM-11 FedRAMP SI-3 FFIEC IS v2016 A.6.17 FFIEC IS v2016 A.8.1(a) IRS Pub 1075 v2016 9.3.17.3 IRS Pub 1075 v2016 9.3.5.11 ISO/IEC 27002:2013 12.2.1 ISO/IEC 27002:2013 12.6.2 ISO/IEC 27799:2016 12.2.1 ISO/IEC 27799:2016 12.6.2 MARS-E v2 CM-11 MARS-E v2 PE-2 MARS-E v2 SI-3 NIST Cybersecurity Framework v1.1 DE.CM-4 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.AT-1

	NIST SP 800-53 R4 SC-27[S]{0} NIST SP 800-53 R4 SC-29[S]{0} NIST SP 800-53 R4 SI-3(4)[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 AC-17.IS3b[M]-0 NY DOH SSP v3.1 CM-11a[M]-2 NY DOH SSP v3.1 SC-7.IS4a[M]-1 PCI DSS v3.2.1 5.1 PCI DSS v3.2.1 5.1.1 PCI DSS v3.2.1 5.2

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 1 Subject to CMMC Level 3 Subject to Community Supplemental Requirements 002 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to HIPAA Security Rule Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Basic Level Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to Supplemental Requirements Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: Critical system file scans are performed during system boot and every 12 hours. Malicious code is blocked and quarantined, and an alert is sent to administrators in response to malicious code detection. The organization addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Malicious code protection mechanisms are centrally managed. For systems considered to be not commonly affected by malicious software, the organization performs periodic assessments to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.

	The organization: 1. employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; 2. implements spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages transported by email, email attachments, web accesses, or other common means; 3. automatically updates malicious code and spam protection mechanisms (including signature definitions) when new releases are available in accordance with the organization's configuration management policy and procedures; 4. configures malicious code protection mechanisms to perform periodic scans of the information system according to organization guidelines and real-time scans of files from external sources at either endpoints or network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and blocks malicious code, quarantine malicious code, or sends alerts to administrator in response to malicious code detection; and 5. addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Malicious code and spam protection mechanisms are centrally managed. User functionality (including user interface services [e.g., web services]) is separated from information system management (e.g., database management systems) functionality. The information system must implement safeguards to protect its memory from unauthorized code execution.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.308(a)(5)(ii)(B) HIPAA.SR-0 AICPA 2017 CC6.8 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CIS CSC v7.1 8.1 CIS CSC v7.1 8.3 CMMC v1.0 SC.3.181-0 CMMC v1.0 SI.1.211-0 CMMC v1.0 SI.1.212-0 CMMC v1.0 SI.1.213-0 CMMC v1.0 SI.3.218-0 CMSRs v3.1 CM-11 (HIGH; MOD) CMSRs v3.1 SC-02 (HIGH; MOD) CMSRs v3.1 SI-03 (HIGH) CMSRs v3.1 SI-03 (HIGH; MOD) CMSRs v3.1 SI-03(01) (HIGH; MOD) CMSRs v3.1 SI-03(02) (HIGH; MOD) CMSRs v3.1 SI-08 (HIGH; MOD) CMSRs v3.1 SI-08(01) (HIGH; MOD) CMSRs v3.1 SI-08(02) (HIGH; MOD) COBIT 5 DS5.9 COBIT 5 DSS05.01 CSA CCM v3.0.1 TVM-01 CSR002 v2018 5.3-0-0 CSR002 v2018 5.4-0-1 FedRAMP SC-2 FedRAMP SI-3 FedRAMP SI-3(1) FedRAMP SI-3(2) FedRAMP SI-8 FedRAMP SI-8(1) FedRAMP SI-8(2) FFIEC IS v2016 A.6.17 FFIEC IS v2016 A.8.1(a) IRS Pub 1075 v2016 9.3.16.2 IRS Pub 1075 v2016 9.3.17.10 IRS Pub 1075 v2016 9.3.17.3

	IRS Pub 1075 v2016 9.3.17.6 IRS Pub 1075 v2016 9.3.5.11 IRS Pub 1075 v2016 9.4.3 ISO/IEC 27002:2013 12.2.1 ISO/IEC 27799:2016 12.2.1 MARS-E v2 DM-2 MARS-E v2 SC-2 MARS-E v2 SI-16 MARS-E v2 SI-3 MARS-E v2 SI-3(1) MARS-E v2 SI-3(2) MARS-E v2 SI-7(7) MARS-E v2 SI-8 MARS-E v2 SI-8(1) NIST 800-171 r2 3.13.3-0 NIST 800-171 r2 3.14.2-0 NIST 800-171 r2 3.14.4-0 NIST 800-171 r2 3.14.5-0 NIST Cybersecurity Framework v1.1 DE.CM-4 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST SP 800-53 R4 AC-4(5)[S]{1} NIST SP 800-53 R4 SC-2(1)[S]{0} NIST SP 800-53 R4 SC-2[HM]{0} NIST SP 800-53 R4 SC-3(2)[S]{0} NIST SP 800-53 R4 SC-3(3)[S]{0} NIST SP 800-53 R4 SC-35[S]{0} NIST SP 800-53 R4 SC-7(13)[S]{0} NIST SP 800-53 R4 SI-16[HM]{0} NIST SP 800-53 R4 SI-3(1)[HM]{0} NIST SP 800-53 R4 SI-3a[HML]{0} NIST SP 800-53 R4 SI-3b[HML]{0} NIST SP 800-53 R4 SI-3c[HML]{0} NIST SP 800-53 R4 SI-3d[HML]{0} NIST SP 800-53 R4 SI-7(3)[S]{0} NIST SP 800-53 R4 SI-8(1)[HM]{0} NIST SP 800-53 R4 SI-8(3)[S]{0} NIST SP 800-53 R4 SI-8a[HM]{0} NIST SP 800-53 R4 SI-8b[HM]{0} NRS 603A.215.1 NY DOH SSP v3.1 AC-17.IS3d[M]-0 NY DOH SSP v3.1 SC-2[M]-0 NY DOH SSP v3.1 SC-7.IS4[M]-2 NY DOH SSP v3.1 SI-16[M]-0 NY DOH SSP v3.1 SI-3(1)[M]-0 NY DOH SSP v3.1 SI-3a[M]-1 NY DOH SSP v3.1 SI-3a[M]-2 NY DOH SSP v3.1 SI-3c1[M]-1 NY DOH SSP v3.1 SI-3c2[M]-0 NY DOH SSP v3.1 SI-3d[M]-0 NY DOH SSP v3.1 SI-8(1)[M]-0 NY DOH SSP v3.1 SI-8a[M]-0 NY DOH SSP v3.1 SI-8b[M]-0 PCI DSS v3.2.1 5.1.2 PCI DSS v3.2.1 5.2 PCI DSS v3.2.1 5.3 SR v6.4 25a-0

Level CIS Implementation Requirements

Level CIS Implementation:	The organization implements the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver-side verification in mail servers to lower the chance of spoofed email messages. The organization enables anti-exploitation features (e.g., Data Execution Prevention [DEP] and Address Space Layout Randomization [ASLR]) in its operating systems and applies anti-exploitation protections to a broader set of applications and executables by deploying additional capabilities, such as the Enhanced Migration Experience Toolkit. The requirements are fully assessed by the organization prior to implementation due to potential difficulties (compatibility issues, etc.).

Level CMMC Implementation Requirements	
Level CMMC Implementation:	The organization employs advanced analytics to test untrusted code and/or programs traversing through the network or system boundaries, in order to detect and block malicious content.

Level CMS Implementation Requirements	
Level CMS Implementation:	Desktop malicious code scanning software is configured to perform critical system file scans every 12 hours.

Level Community Supplemental Reqs 02 Implementation Requirements	
Level Community Supplemental Reqs 02 Implementation:	The organization augments endpoint protection strategies with additional solutions—including those built into the operating system if available—to mitigate exploitation of unknown vulnerabilities where traditional antivirus may be ineffective; and where applicable, target the solutions to protect commonly exploited applications (e.g., web browsers, office productivity suites, Java plugins).

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation:	The organization implements non-signature based malicious code detection mechanisms to provide safeguards against malicious code for which signatures do not yet exist or for which existing signatures may not be effective.

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation:	The agency must: 1. Establish policies governing the installation of software by users; 2. Enforce software installation policies through automated methods; and 3. Monitor policy compliance on a continual basis. Implement malware protection at one or more points within the email delivery process to protect against viruses, worms, and other forms of malware. The agency must configure virtualized desktops to provide the functionalities only required for operations, non-essential functionality, or components must be removed or prohibited.

Level HIX Implementation Requirements	
Level HIX Implementation:	Desktop malicious code scanning software is configured to perform critical system file scans every 24 hours.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation:	Malicious code scanning software on servers (to include databases and applications) is configured to perform critical system file scans no less often than once every twelve [12] hours and full system scans no less often than once every seventy-two [72] hours.

	The information system automatically updates spam protection mechanisms. The organization updates malicious code protection mechanisms whenever new releases are available in accordance with CMS configuration management policy and procedures.

Control Reference: 09.k Controls Against Mobile Code

Control Specification:	Mobile code shall be authorized before its installation and use, and the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy. All unauthorized mobile code shall be prevented from executing. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Authorization; Cryptography; Policies and Procedures; Viruses and Malware

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to Community Supplemental Requirements 002
Level 1 Implementation:	Automated controls (e.g., browser settings) are in place to authorize and restrict the use of mobile code (e.g., Java, JavaScript, ActiveX, PDF, postscript, Shockwave movies, and Flash animations). A formal policy is in place for mobile code protection and to ensure protective measures, including anti-virus and anti-spyware, are in place and regularly updated.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 SC-18 (HIGH; MOD) CMSRs v3.1 SI-03 (HIGH) CSA CCM v3.0.1 TVM-01 CSA CCM v3.0.1 TVM-03 CSR002 v2018 5.4-0-2 FedRAMP SI-3 FFIEC IS v2016 A.6.17 IRS Pub 1075 v2016 9.3.16.12 IRS Pub 1075 v2016 9.3.17.3 ISO/IEC 27002:2013 12.2.1 ISO/IEC 27799:2016 12.2.1 MARS-E v2 SC-18 MARS-E v2 SI-3 NIST Cybersecurity Framework v1.1 DE.CM-4 NIST Cybersecurity Framework v1.1 DE.CM-5

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions

	Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CMMC Level 3 Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The organization formally addresses controls (e.g., policies and procedures) for blocking any use and receipt (e.g., downloading and execution) of mobile codes. The following actions are carried out to protect against mobile code performing unauthorized actions: 1. ensuring a logically isolated environment is established for executing mobile code; 2. activating technical measures as available on a specific system to ensure mobile code is managed; and 3. controlling the resources with access to mobile code.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC8.1 CMMC v1.0 SC.3.188-0 CMSRs v3.1 CM-03 (HIGH; MOD) CMSRs v3.1 SC-02 (HIGH) CMSRs v3.1 SC-03 (HIGH) CMSRs v3.1 SC-18 (HIGH) CRR v2016 VM:G1.Q4 CSA CCM v3.0.1 TVM-03 FedRAMP CM-3 FedRAMP SC-18 FedRAMP SC-2 FFIEC IS v2016 A.6.17 IRS Pub 1075 v2016 9.3.16.12 IRS Pub 1075 v2016 9.3.16.2 IRS Pub 1075 v2016 9.3.5.3 ISO/IEC 27002:2013 12.2.1 ISO/IEC 27002:2013 12.5.1 ISO/IEC 27799:2016 12.2.1 ISO/IEC 27799:2016 12.5.1 MARS-E v2 CM-3 MARS-E v2 SC-18 MARS-E v2 SC-2 NIST 800-171 r2 3.13.13-0 NIST Cybersecurity Framework v1.1 DE.CM-5 NIST Cybersecurity Framework v1.1 PR.DS-7

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The organization (i) defines acceptable and unacceptable mobile code and mobile code technologies; (ii) establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and (iii) authorizes, monitors, and controls the use of mobile code within the information system.

Objective Name: 09.05 Information Back-Up

Control Objective:	Ensure the maintenance, integrity, and availability of organizational information.

Control Reference: 09.l Back-up

Control Specification:	Back-up copies of information and software shall be taken and tested regularly. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Cryptography; Documentation and Records; Physical and Facility Security; Policies and Procedures; Third-parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 2 Subject to HIPAA Security Rule Subject to Joint Commission Accreditation Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to Texas Health and Safety Code
Level 1 Implementation:	Back-up copies of information and software are made, at appropriate intervals, and when equipment is moved (relocated), and tested regularly in accordance with an agreed-upon back-up policy. A formal definition of the level of back-up required for each system is defined and documented including the scope of data to be imaged, frequency of imaging, and duration of retention. This is based on the contractual, legal, regulatory and business requirements. Complete restoration procedures are defined and documented for each system. The back-ups are stored in a physically secure remote location, at a sufficient distance to make them reasonably immune from damage to data at the primary site. Physical and environmental controls are in place for the back-up copies. The organization ensures that backups, including remote and cloud-based backups, are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. Regular testing of back-up media and restoration procedures is performed. Inventory records for the back-up copies, including content and current location, are maintained. When the back-up service is delivered by the third-party, the service level agreement includes the detailed protections to control confidentiality, integrity, and availability of the back-up information.

	Workforce members roles and responsibilities in the data backup process for Bring Your Own Device (BYOD) are identified and communicated to the workforce; in particular, users are required to perform backups of organizational and/or client data on their BYOD device(s).
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.308(a)(7)(ii)(A) HIPAA.SR-0 45 CFR Part § 164.310(d)(2)(iv) HIPAA.SR-1 AICPA 2017 A1.2 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CIS CSC v7.1 10.3 CIS CSC v7.1 10.4 CMMC v1.0 RE.2.137-0 CMSRs v3.1 CP-02 (HIGH; MOD) CMSRs v3.1 CP-06 (HIGH; MOD) CMSRs v3.1 CP-09 (HIGH; MOD) CMSRs v3.1 CP-09(01) (HIGH; MOD) CMSRs v3.1 CP-09(02) (HIGH) CMSRs v3.1 MP-04 (HIGH; MOD) CMSRs v3.1 MP-05 (HIGH; MOD) CRR v2016 AM:G6.Q5 CRR v2016 SCM:G3.Q4 CSA CCM v3.0.1 BCR-11 CSA CCM v3.0.1 MOS-17 FedRAMP CP-2 FedRAMP CP-9 FedRAMP CP-9(1) FedRAMP MP-4 IRS Pub 1075 v2016 4.2 IRS Pub 1075 v2016 4.4 IRS Pub 1075 v2016 4.5 IRS Pub 1075 v2016 9.3.10.3 IRS Pub 1075 v2016 9.3.10.5 IRS Pub 1075 v2016 9.3.6.2 IRS Pub 1075 v2016 9.3.6.5 IRS Pub 1075 v2016 9.3.6.7 IRS Pub 1075 v2016 9.4.14 ISO/IEC 27002:2013 12.3.1 ISO/IEC 27002:2013 15.2 ISO/IEC 27799:2016 12.3.1 ISO/IEC 27799:2016 15.2 MARS-E v2 CP-2 MARS-E v2 CP-6 MARS-E v2 CP-9 MARS-E v2 CP-9(1) MARS-E v2 MP-4 MARS-E v2 MP-5 NIST Cybersecurity Framework v1.1 ID.SC-5 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.IP-4 NIST SP 800-53 R4 CP-10(6)[S]{0} NIST SP 800-53 R4 CP-9[HML]{1} NRS 603A.215.1 NY DOH SSP v3.1 CP-9.IS2[M]-1 NY DOH SSP v3.1 CP-9d[M]-0 OCR Audit Protocol (2016) 164.310(d)(2)(iv) PCI DSS v3.2.1 9.5.1 PMI DSP Framework RC-1 TJC IM.01.01.03, EP 4

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions

	Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 2 Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the EU GDPR
Level 2 Implementation:	Level 1 plus: Automated tools track all back-ups. The integrity and security of the backup copies are maintained to ensure future availability in accordance with the agreed backup policy. To mitigate the risk of attacks that seek to encrypt or damage data on addressable data shares, including backup destinations, the organization provides key systems with at least one backup destination that is not continuously addressable through operating system calls. Any potential accessibility problems with the back-up copies are identified and mitigated in the event of an area-wide disaster. Covered and/or confidential information is backed-up in an encrypted format to guarantee confidentiality.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 A1.2 CIS CSC v7.1 10.5 CMMC v1.0 RE.2.138-0 CMSRs v3.1 CP-06(03) (HIGH; MOD) CMSRs v3.1 CP-09 (HIGH; MOD) CMSRs v3.1 SC-28 (HIGH; MOD) CSA CCM v3.0.1 EKM-03 FedRAMP SC-28 IRS Pub 1075 v2016 4.2 IRS Pub 1075 v2016 4.5 IRS Pub 1075 v2016 9.3.16.15 IRS Pub 1075 v2016 9.3.6.7 IRS Pub 1075 v2016 9.4.11 IRS Pub 1075 v2016 9.4.14 ISO/IEC 27002:2013 12.3.1 ISO/IEC 27799:2016 12.3.1 MARS-E v2 CP-6(3) MARS-E v2 CP-9 MARS-E v2 SC-28 NIST 800-171 r2 3.8.9-0 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.IP-4 NIST SP 800-53 R4 CP-9[HML]{2} NY DOH SSP v3.1 CP-6(3)[M]-0 NY DOH SSP v3.1 CP-9.IS2[M]-2

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB)

	Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to CMMC Level 3 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to HIPAA Security Rule Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: The organization performs full backups weekly to separate media. Incremental or differential backups are performed daily to separate media. Three generations of backups (full plus all related incremental or differential backups) are stored off site. Off-site and on-site backups are logged with name, date, time, and action. The organization ensures a current, retrievable copy of covered information is available before movement of servers. The organization tests backup information following each backup to verify media reliability and information integrity, at least annually.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.310(d)(2)(iv) HIPAA.SR-2 AICPA 2017 A1.3 CMMC v1.0 RE.3.139-0 CMSRs v3.1 CP-09 (HIGH; MOD) CMSRs v3.1 CP-09(01) (HIGH; MOD) CMSRs v3.1 CP-09(03) (HIGH) CMSRs v3.1 CP-09(05) (HIGH) FedRAMP CP-9(1) IRS Pub 1075 v2016 4.2 IRS Pub 1075 v2016 4.4 IRS Pub 1075 v2016 4.5 IRS Pub 1075 v2016 9.3.10.3 IRS Pub 1075 v2016 9.3.6.7 IRS Pub 1075 v2016 9.4.11 IRS Pub 1075 v2016 9.4.14 ISO/IEC 27002:2013 12.3.1 ISO/IEC 27799:2016 12.3.1 MARS-E v2 CP-9 MARS-E v2 CP-9(1) NIST Cybersecurity Framework v1.1 PR.IP-4 NIST SP 800-53 R4 CP-9(1)[HM]{0} NY DOH SSP v3.1 CP-9(6)[MN]-2 NY DOH SSP v3.1 CP-9.IS.PHI1[M]-0 NY DOH SSP v3.1 CP-9.IS1[M]-1 NY DOH SSP v3.1 CP-9.IS1[M]-3 NY DOH SSP v3.1 CP-9a[M]-2 NY DOH SSP v3.1 CP-9a[M]-3 NY DOH SSP v3.1 CP-9b[M]-2 NY DOH SSP v3.1 CP-9b[M]-3

Level CIS Implementation Requirements

Level CIS Implementation:	The organization automatically backs up each system on a regular basis and ensures that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.

Level CMS Implementation Requirements

Level CMS Implementation:	Backups include: 1. copies of user-level and system-level information (including system state information); 2. copies of the operating system and other critical information system software; and 3. the information system inventory (including hardware, software, and firmware components). The organization transfers information system backup information to the alternate storage site at defined time periods (defined in the applicable security plan) and transfer rates (defined in the applicable security plan) consistent with the recovery time and recovery point objectives.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The service provider determines what elements of the cloud environment require the Information System Backup control determines how Information System Backup is going to be verified and appropriate periodicity of the check. The service provider maintains at least three backup copies of user-level information, system-level information, and information system documentation (at least one of which is available online) or provides an equivalent alternative. The organization stores backup copies of organization-defined critical information system software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the operational system.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	Back-up tapes must be labeled as containing FTI, must be logged, must be transported securely using two barriers and a transmittal, and must be inventoried on a semi-annual basis. The organization protects the confidentiality of backup information at storage locations pursuant to IRC 6013. Backups (virtual machine snapshot) must be properly secured and must be stored in a logical location where the backup is only accessible to those with a need-to-know.

Level HIX Implementation Requirements

Level HIX Implementation:	The organization ensures a current, retrievable copy of Personally Identifiable Information (PII) is available before the movement of servers.

	For cloud environments, the system owner determines what elements of the cloud environment require backups and how backups will be verified and the appropriate periodicity of the check.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation:	The organization tests backup information following each backup, at least every six [6] months for Moderate systems, to verify media reliability and information integrity.

Level Title 23 NYCRR Part 500 Implementation Requirements	
Level Title 23 NYCRR Part 500 Implementation:	The covered entity maintains backups of systems designed to reconstruct material financial transactions to support normal operations and obligations of the covered entity for five years.

Objective Name: 09.06 Network Security Management

Control Objective:	Ensure the protection of information in networks and protection of the supporting network infrastructure.

Control Reference: 09.m Network Controls

Control Specification:	Networks shall be managed and controlled in order to protect the organization from threats and to maintain security for the systems and applications using the network, including information in transit. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Authentication; Communications and Transmissions; Cryptography; Data Loss Prevention; Monitoring; Network Security

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 3 Subject to Community Supplemental Requirements 002 Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Supplemental Requirements Subject to Texas Health and Safety Code
Level 1 Implementation:	Network managers implement controls to ensure the security of information in networks, and the protection of connected services from unauthorized access. Controls are implemented to ensure the availability of network services and information services

	using the network. Responsibilities and procedures are established for the management of equipment on the network, including equipment in user areas. When configuring wireless access points and devices, the organization changes the following: 1. vendor default encryption keys; 2. encryption keys anytime anyone with knowledge of the keys leaves the company or changes positions; 3. default SNMP community strings on wireless devices; 4. default passwords/passphrases on access points; 5. other security-related wireless vendor defaults, if applicable. A current network diagram (for example, one that shows how covered information flows over the network) exists, documenting all connections to systems storing, processing or transmitting covered information, including any wireless networks. Network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts. Review and update the network diagram as based on the changes in the environment and no less than every six months. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols can be continued targets of malicious individuals who exploit these vulnerabilities to gain privileged access to covered information environments. The organization monitors for all authorized and unauthorized wireless access to the information system and prohibits installation of wireless access points (WAP) unless explicitly authorized, in writing, by the CIO or his/her designated representative. If wireless access is explicitly approved, wireless access points and devices have appropriate (e.g., FIPS-approved; minimum of AES WPA2) encryption enabled for authentication and transmission. WAPs are placed in secure areas.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CIS CSC v7.1 15.1 CIS CSC v7.1 15.2 CIS CSC v7.1 15.7 CMMC v1.0 AC.3.012-1 CMSRs v3.1 AC-18 (HIGH; MOD) CMSRs v3.1 AC-18(01) (HIGH; MOD) CMSRs v3.1 SI-04 (HIGH; MOD) CRR v2016 AM:G2.Q5 CRR v2016 CM:G2.Q2 CRR v2016 CM:G2.Q4 CRR v2016 CM:G2.Q8 CSA CCM v3.0.1 IVS-06 CSA CCM v3.0.1 IVS-12 CSA CCM v3.0.1 IVS-13 CSR002 v2018 11.1-0-0 CSR002 v2018 11.1-0-1 CSR002 v2018 11.3-0-1 FedRAMP AC-18 FedRAMP AC-18(1) FedRAMP SI-4 FFIEC IS v2016 A.6.10 FFIEC IS v2016 A.6.7(a) FFIEC IS v2016 A.6.7(b) FFIEC IS v2016 A.6.7(c) IRS Pub 1075 v2016 9.3.1.13 IRS Pub 1075 v2016 9.4.18 ISO/IEC 27002:2013 13.1.1 ISO/IEC 27799:2016 13.1.1 MARS-E v2 AC-18 MARS-E v2 AC-18(1) MARS-E v2 SI-4

	NIST 800-171 r2 3.1.17-1 NIST Cybersecurity Framework v1.1 DE.AE-1 NIST Cybersecurity Framework v1.1 DE.CM-1 NIST Cybersecurity Framework v1.1 ID.AM-3 NIST Cybersecurity Framework v1.1 PR.DS-2 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.IP-1 NIST SP 800-53 R4 SC-40(2)[S]{0} NY DOH SSP v3.1 AC-18(1)[M]-1 PCI DSS v3.2.1 1.1 PCI DSS v3.2.1 1.1.2 PCI DSS v3.2.1 1.1.3 PCI DSS v3.2.1 1.1.4 PCI DSS v3.2.1 11.1 PCI DSS v3.2.1 2.1.1 PCI DSS v3.2.1 4.1.1 PMI DSP Framework PR.DS-1 SR v6.4 11-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions HIE Transactions: More than 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients Hospital Admissions: More than 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Count: Greater than 25 Physicians Physician Encounters: Between 60k to 180k Encounters Physician Encounters: Greater than 180k Encounters Record Count Annual: Between 180k and 725k Records Record Count Annual: More than 725k Records Record Total: Between 10 and 60 Million Records Record Total: More than 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 1 Subject to CMMC Level 2 Subject to CMMC Level 3 Subject to CMMC Level 4 Subject to CMMC Level 5 Subject to Community Supplemental Requirements 002 Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to HIPAA Security Rule Subject to HITRUST De-ID Framework Requirements Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Basic Level Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High)

	Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to Supplemental Requirements Subject to the CMS Minimum Security Requirements (High) Subject to the EU GDPR
Level 2 Implementation:	Level 1 plus: Quarterly network scans are performed to identify unauthorized components/devices. The organization uniquely identifies and authenticates network devices that require authentication mechanisms, before establishing a connection, that, at a minimum, use shared information (i.e., MAC or IP address) and access control lists to control remote network access. To identify and authenticate devices on local and/or wide area networks, including wireless networks, the information system uses either: 1. shared known information solutions (Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses); or 2. an organizational authentication solution (IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication). The required strength of the device authentication mechanism is determined by the security categorization of the information system. A formal process is established for approving and testing all network connections and changes to firewall, router, and switch configurations. Any deviations from the standard configuration or updates to the standard configuration are documented and approved in a change control system. All new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPS, are also documented and recorded, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need. The organization builds a firewall configuration that restricts connections between un-trusted networks and any system components in the covered information environment (Note: An "un-trusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.) Any changes to the firewall configuration are updated in the network diagram. The firewall configuration: 1. restricts inbound and outbound traffic to that which is necessary for the covered information system's environment; 2. secures and synchronizes router configuration files; 3. requires firewalls between any wireless networks and the covered information system's environment; and 4. configures these firewalls to deny or control any traffic from a wireless environment into the covered data environment. The organization ensures information systems protect the confidentiality and integrity of transmitted information, including during preparation for transmission and during reception. The organization requires information systems to use FIPS-validated cryptographic mechanisms during transmission to prevent unauthorized disclosure of information and detect changes to information unless otherwise protected by organization-defined, alternative physical measures.

	Organizations use secured and encrypted communication channels when migrating physical servers, applications, or data to virtualized servers. Usage restrictions and implementation guidance are defined and documented for VoIP, including the authorization and monitoring of the service. Perform quarterly scans for unauthorized wireless access points and take appropriate action if any access points are discovered. The organization: 1. authorizes connections from the information system to other information systems outside of the organization through the use of interconnection security agreements or other formal agreement; 2. documents for each connection, the interface characteristics, security requirements, and the nature of the information communicated; 3. employs a deny-all, permit-by-exception policy for allowing connections from the information system to other information systems outside of the organization; and 4. applies a default-deny rule that drops all traffic via host-based firewalls or port filtering tools on its endpoints (workstations, servers, etc.), except those services and ports that are explicitly allowed.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.312(c)(1) HIPAA.SR-2 45 CFR Part § 164.312(e)(1) HIPAA.SR-1 45 CFR Part § 164.312(e)(2)(i) HIPAA.SR-1 CAQH Core Phase 1 153: Eligibility and Benefits Connectivity Rule v1.1.0 Subsection 5.2 CIS CSC v7.1 11.1 CIS CSC v7.1 11.2 CIS CSC v7.1 11.3 CIS CSC v7.1 11.5 CIS CSC v7.1 12.3 CIS CSC v7.1 13.4 CIS CSC v7.1 15.8 CIS CSC v7.1 9.4 CMMC v1.0 AC.1.003-1 CMMC v1.0 AC.4.023-2 CMMC v1.0 AC.5.024-0 CMMC v1.0 CA.2.157-3 CMMC v1.0 IA.1.076-2 CMMC v1.0 IA.1.077-2 CMMC v1.0 SC.3.185-0 CMMC v1.0 SC.3.189-0 CMSRs v3.1 CA-03 (HIGH; MOD) CMSRs v3.1 CM-03 (HIGH; MOD) CMSRs v3.1 IA-03 (HIGH; MOD) CMSRs v3.1 SC-07 (HIGH; MOD) CMSRs v3.1 SC-07(05) (HIGH; MOD) CMSRs v3.1 SC-08 (HIGH; MOS) CMSRs v3.1 SC-08(01) (HIGH; MOD) CMSRs v3.1 SC-19 (HIGH; MOD) CMSRs v3.1 SC-20 (HIGH; MOD) CMSRs v3.1 SI-04 (HIGH; MOD) CRR v2016 CM:G2.Q2 CRR v2016 CM:G2.Q4 CRR v2016 CM:G2.Q8 CSA CCM v3.0.1 IVS-06 CSA CCM v3.0.1 IVS-10 CSR002 v2018 11.1-0-3 CSR002 v2018 11.2-1-1 CSR002 v2018 11.2-1-2 CSR002 v2018 4.2-1-0 CSR002 v2018 4.2-2-0 De-ID Framework v1 Transmission Encryption: Policies FedRAMP CA-3 FedRAMP CM-3 FedRAMP IA-3 FedRAMP SC-19 FedRAMP SC-7 FedRAMP SC-8 FedRAMP SI-4

FedRAMP SI-4(14)
FFIEC IS v2016 A.6.10
FFIEC IS v2016 A.6.18(d)
FFIEC IS v2016 A.6.7(b)
FFIEC IS v2016 A.6.7(c)
IRS Pub 1075 v2016 9.3.16.13
IRS Pub 1075 v2016 9.3.16.5
IRS Pub 1075 v2016 9.3.16.6
IRS Pub 1075 v2016 9.3.4.3
IRS Pub 1075 v2016 9.3.5.3
IRS Pub 1075 v2016 9.3.7.3
IRS Pub 1075 v2016 9.4.15
IRS Pub 1075 v2016 9.4.18
ISO/IEC 27002:2013 13.1.1
ISO/IEC 27002:2013 13.1.2
ISO/IEC 27002:2013 13.1.3
ISO/IEC 27799:2016 13.1.1
ISO/IEC 27799:2016 13.1.2
ISO/IEC 27799:2016 13.1.3
MARS-E v2 CA-3
MARS-E v2 CM-3
MARS-E v2 IA-3
MARS-E v2 SC-19
MARS-E v2 SC-20
MARS-E v2 SC-7
MARS-E v2 SC-7(5)
MARS-E v2 SC-8
MARS-E v2 SC-8(1)
MARS-E v2 SC-9
MARS-E v2 SC-9(1)
MARS-E v2 SI-4
MARS-E v2 SI-4(14)
NIST 800-171 r2 3.1.20-1
NIST 800-171 r2 3.12.4-3
NIST 800-171 r2 3.13.14-0
NIST 800-171 r2 3.13.8-0
NIST 800-171 r2 3.5.1-2
NIST 800-171 r2 3.5.2-2
NIST Cybersecurity Framework v1.1 DE.AE-1
NIST Cybersecurity Framework v1.1 DE.CM-1
NIST Cybersecurity Framework v1.1 PR.AC-1
NIST Cybersecurity Framework v1.1 PR.AC-5
NIST Cybersecurity Framework v1.1 PR.DS-2
NIST SP 800-53 R4 AC-18(1)[HM]{1}
NIST SP 800-53 R4 CA-3a[HML]{0}
NIST SP 800-53 R4 CA-9(1)[S]{0}
NIST SP 800-53 R4 CA-9[HML]{0}
NIST SP 800-53 R4 IA-3(1)[S]{1}
NIST SP 800-53 R4 IA-3(4)[S]{0}
NIST SP 800-53 R4 IA-3[HM]{0}
NIST SP 800-53 R4 IA-5(6)[S]{0}
NIST SP 800-53 R4 IA-9(2)[S]{0}
NIST SP 800-53 R4 IA-9[S]{1}
NIST SP 800-53 R4 SA-4(6)a[S]{1}
NIST SP 800-53 R4 SA-4(7)b[S]{0}
NIST SP 800-53 R4 SC-16(1)[S]{0}
NIST SP 800-53 R4 SC-19[HM]{0}
NIST SP 800-53 R4 SC-28(1)[S]{0}
NIST SP 800-53 R4 SC-40(4)[S]{0}
NIST SP 800-53 R4 SC-7(4)c[HM]{0}
NIST SP 800-53 R4 SC-8(1)[HM]{0}
NIST SP 800-53 R4 SC-8(2)[S]{0}
NIST SP 800-53 R4 SC-8(3)[S]{0}
NIST SP 800-53 R4 SC-8[HM]{0}
NY DOH SSP v3.1 AC-4[M]-2
NY DOH SSP v3.1 CA-3(5)[M]-0
NY DOH SSP v3.1 CA-3.IS5[HML]-0
NY DOH SSP v3.1 CA-3a[M]-0
NY DOH SSP v3.1 CA-3b[M]-0
NY DOH SSP v3.1 CA-3d[M]-0
NY DOH SSP v3.1 CA-9b[M]-0
NY DOH SSP v3.1 CM-7b[M]-2
NY DOH SSP v3.1 IA-2.IS1[M]-1
NY DOH SSP v3.1 IA-3[M]-0
NY DOH SSP v3.1 SC-19a[M]-0

	NY DOH SSP v3.1 SC-19b[M]-0 NY DOH SSP v3.1 SC-7(4)c[M]-0 NY DOH SSP v3.1 SC-7.IS1[M]-0 NY DOH SSP v3.1 SC-8(1).PII[M]-0 PCI DSS v3.2.1 1.1.1 PCI DSS v3.2.1 1.1.3 PCI DSS v3.2.1 1.2 PCI DSS v3.2.1 1.2.2 PCI DSS v3.2.1 1.2.3 PCI DSS v3.2.1 11.1 SR v6.4 10.4-0 SR v6.4 42.2-0 SR v6.4 45a-1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to Banking Requirements Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 1 Subject to CMMC Level 2 Subject to CMMC Level 5 Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Basic Level Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to Supplemental Requirements Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: An analysis is conducted to determine the impact the loss of network service availability will have upon critical business functions. Technical controls are implemented to safeguard the confidentiality and integrity of covered information passing over the organization's network and to/from public networks. Technical tools and solutions are implemented and used to identify the vulnerabilities and mitigate the threats, including intrusion detection system (IDS) and/or intrusion prevention systems (IPS), and vulnerability scanning. The organization employs tools and techniques, such as an IDS and IPS, to monitor events on the information system, detects and responds to attacks, and provides identification of unauthorized use of the system. These tools are implemented at the perimeter of the

organization's environment and at key points within the environment, including IDS and IPS deployed on the wireless side of the firewall (WIDS) to identify rogue wireless devices, monitor all traffic to and from the wireless segment, and detect attack attempts and successful compromises. These tools are updated on a regular basis, including the engines, the baselines, and signatures.

Management processes are implemented to ensure coordination of, and consistency in, the elements of the network infrastructure.

The organization establishes firewall and router configuration standards for the current network with all connections to covered information, including any wireless networks. A description of groups, roles, and responsibilities for the logical management of network components is documented.

Documentation and business justification are provided for the use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. The firewall and router rule sets are reviewed at least every six months.

Wireless access points are shut down when not in use (e.g., nights, weekends). MAC address authentication and static IP addresses are utilized. Access points are placed in secure areas. File sharing is disabled on all wireless clients.

The router configuration files are secured and synchronized. Access to all proxies is denied, except for those hosts, ports, and services that are explicitly required. The organization utilizes firewalls from at least two different vendors at the various levels within the network to reduce the possibility of compromising the entire network.

The organization prohibits direct public access between the Internet and any system component in the covered data environment.

This is achieved by performing the following:

1. establishing DMZ to limit inbound and outbound traffic to only protocols that are necessary for the covered data environment;
2. limiting inbound Internet traffic to IP addresses within the DMZ;
3. not allowing any direct routes inbound or outbound for traffic between the Internet and the covered data environment;
4. not allowing internal addresses to pass from the Internet into the DMZ;
5. restricting outbound traffic from the covered data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ;
6. implementing stateful inspection, also known as dynamic packet filtering (that is, only "established" connections are allowed into the network);
7. placing all database(s), servers and other system components storing or processing covered information in an internal network zone, segregated from the DMZ;
8. methods including, but not limited to, Network Address Translation (NAT), placing system components behind a proxy server, and/or removing or filtering route advertisements; and
9. web servers must reside in a DMZ and application and database servers must reside in trusted internal networks.

To eliminate single points of failure and to enhance redundancy, there are at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. These servers are located on different subnets and geographically separated. Authoritative DNS servers are segregated into internal and external roles. The DNS server with the internal role provides name/address resolution information pertaining to both internal and external information technology resources while the DNS server with the external role only provides name/address resolution information pertaining to external information technology resources.

Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CIS CSC v7.1 1.7 CIS CSC v7.1 11.1 CIS CSC v7.1 12.5 CIS CSC v7.1 12.6 CIS CSC v7.1 12.7 CMMC v1.0 SC.1.175-2 CMMC v1.0 SC.5.198-0 CMMC v1.0 SI.2.216-0 CMSRs v3.1 AC-18 (HIGH; MOD) CMSRs v3.1 AC-18(01) (HIGH; MOD) CMSRs v3.1 AC-18(04) (HIGH) CMSRs v3.1 AC-18(05) (HIGH) CMSRs v3.1 AR-05 (HIGH; MOD) CMSRs v3.1 CM-07 (HIGH; MOD) CMSRs v3.1 CP-02 (HIGH; MOD) CMSRs v3.1 SC-07 (HIGH; MOD) CMSRs v3.1 SC-07(05) (HIGH; MOD) CMSRs v3.1 SC-07(18) (HIGH) CMSRs v3.1 SC-22 (HIGH; MOD) CMSRs v3.1 SC-7(18) (HIGH) CMSRs v3.1 SI-04 (HIGH; MOD) COBIT 5 DS5.10 COBIT 5 DSS05.02 CRR v2016 CM:G2.Q8 FedRAMP AC-18 FedRAMP AC-18(1) FedRAMP CM-7 FedRAMP CP-2 FedRAMP SC-22 FedRAMP SC-7 FedRAMP SI-4 FedRAMP SI-4(14) FFIEC IS v2016 A.8.1(a) FFIEC IS v2016 A.8.1(h) FFIEC IS v2016 A.8.4 IRS Pub 1075 v2016 9.3.1.13 IRS Pub 1075 v2016 9.3.5.7 IRS Pub 1075 v2016 9.3.6.2 IRS Pub 1075 v2016 9.4.1.8 IRS Pub 1075 v2016 9.4.10 IRS Pub 1075 v2016 9.4.11 IRS Pub 1075 v2016 9.4.14 IRS Pub 1075 v2016 9.4.17 IRS Pub 1075 v2016 9.4.18 IRS Pub 1075 v2016 Exhibit 10 ISO/IEC 27002:2013 13.1.1 ISO/IEC 27002:2013 13.1.3 ISO/IEC 27799:2016 13.1.1 ISO/IEC 27799:2016 13.1.3 MARS-E v2 AC-18 MARS-E v2 AC-18(1) MARS-E v2 AR-5 MARS-E v2 CM-7 MARS-E v2 CP-2 MARS-E v2 PM-1 MARS-E v2 SC-22 MARS-E v2 SC-7 MARS-E v2 SC-7(5) MARS-E v2 SI-4 NIST 800-171 r2 3.13.1-2 NIST 800-171 r2 3.14.6-0 NIST Cybersecurity Framework v1.1 DE.AE-1 NIST Cybersecurity Framework v1.1 DE.AE-4 NIST Cybersecurity Framework v1.1 DE.CM-1 NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.AC-5 NIST SP 800-53 R4 AC-18(3)[S]{0} NIST SP 800-53 R4 SC-7(3)[HM]{0} NIST SP 800-53 R4 SI-4(15)[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 SC-7.IS2[M]-0 NY DOH SSP v3.1 SC-7.IS4b[M]-1 NY DOH SSP v3.1 SC-7.IS4c[M]-0 NY DOH SSP v3.1 SI-4.IS1[HML]-0

	NY DOH SSP v3.1 SI-4a1[M]-0 NY DOH SSP v3.1 SI-4c2[M]-0 PCI DSS v3.2.1 1.1.4 PCI DSS v3.2.1 1.1.6 PCI DSS v3.2.1 1.1.7 PCI DSS v3.2.1 1.2.2 PCI DSS v3.2.1 1.3 PCI DSS v3.2.1 1.3.1 PCI DSS v3.2.1 1.3.2 PCI DSS v3.2.1 1.3.3 PCI DSS v3.2.1 1.3.4 PCI DSS v3.2.1 1.3.5 PCI DSS v3.2.1 1.3.6 PCI DSS v3.2.1 1.3.7 PCI DSS v3.2.1 1.3.8 PCI DSS v3.2.1 11.4 PCI DSS v3.2.1 9.1.3 SR v6.4 10.3-0 SR v6.4 4-0

Level CIS Implementation Requirements

Level CIS Implementation:	Where a specific business need for wireless access has been identified, the organization configures wireless access on client machines to allow access only to authorized wireless networks. For devices that do not have an essential wireless business purpose, the organization disables wireless access in the hardware configuration (basic input/output system or extensible firmware interface). The organization maintains and enforces network-based URL filters that limit a system's ability to connect to websites not approved by the organization. The organization specifically blocks access to known file transfer and email exfiltration websites. The organization subscribes to URL categorization services to ensure that they are up to date with the most recent website category definitions available. Uncategorized sites are blocked by default. This filtering is enforced for each of the organization's systems, whether they are physically at an organization's facilities or not. The organization denies communications with (or limit data flow to) known malicious or unused IP addresses (blacklists), and limit access only to trusted sites (whitelists). The organization enables DNS query logging to detect hostname lookup for known malicious command and control domains.

Level CMMC Implementation Requirements

Level CMMC Implementation:	The organization uses encrypted sessions for the management of network devices.

Level CMS Implementation Requirements

Level CMS Implementation:	The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities. The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries. The organization prohibits the use of Voice over Internet Protocol (VoIP) technologies, unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative. If VoIP is authorized, the organization ensures VoIP equipment used to transmit or discuss sensitive information is protected with FIPS 140-2 encryption standards.

Level Community Supplemental Reqs 02	Implementation Requirements
Level Community Supplemental Reqs 02 Implementation:	The organization utilizes a hardened intermediary system, running only a pre-defined set of applications (without Internet access or office productivity applications), to: i) prevent end-users from directly communicating to administrative network zones; and ii) control privileged access for administrators, developers, and others who need greater network access than regular end-users, to perform their job duties. The organization restricts communication with administrative network zones using a deny-by-default and allow-by-exception policy for all ports, protocols, and services, including the use of administrative interfaces from intentionally published services that may allow unauthorized information access. The organization protects workstations from potentially-compromised peers by: i) blocking inbound communication from other workstations to prevent network traffic between workstations (e.g., using host-based firewalls); and ii) allowing only communication from administrative services (e.g., configuration management, domain controllers, remote support systems). Exceptions are approved on a limited basis to specific sources and destinations. The organization develops a capability for capturing and retaining network traffic and/or network flows at key points in the network and between different trust zones to support dependent operational processes, while managing associated costs. The organization employs a mechanism to aggregate and retain network traffic flows (as appropriate, based on risks and regulations) in a searchable repository, which can be used to support alerting, response, investigation, and forensics processes, including reconstructing artifacts and indexing packet captures for analyses. The system scans and inspects inbound payloads in its entirety, using sandboxing or malware detonation technologies to detect and block malicious content, prior to reaching endpoints. The system (i) controls the domain name system (DNS) infrastructure by using enterprise-managed DNS servers; (ii) systematically identifies and blocks traffic to malicious domain names (blackholing); and (iii) redirects blackholed domains to a non-routable address or other specified destination for monitoring.

Level Federal	Implementation Requirements
Level Federal Implementation:	The information system provides: 1. additional data origin integrity artifacts (e.g., digital signatures, cryptographic keys) along with authoritative data (e.g., DNS resource records) in response queries to obtain origin authentication and integrity verification assurances; and 2. the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace. The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources. A resolving or caching domain name system (DNS) server and authoritative DNS servers are examples of systems that perform this function.

Level FedRAMP	Implementation Requirements

Level FedRAMP Implementation:	The information system provides: 1. additional data origin integrity artifacts (e.g., digital signatures, cryptographic keys) along with authoritative data (e.g., DNS resource records) in response queries to obtain origin authentication and integrity verification assurances; 2. the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace. The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources. A resolving or caching domain name system (DNS) server and authoritative DNS servers are examples of systems that perform this function. The information system fails securely in the event of an operational failure of a boundary protection device. The organization uses cryptographic mechanisms during transmission to prevent unauthorized disclosure of information and detect changes to information unless otherwise protected by a hardened or alarmed carrier Protective Distribution System (PDS).

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	Intrusion detection software is installed and maintained to monitor networks for any unauthorized attempt to access tax data in a data warehousing environment. The agency identifies and analyzes how FTI in a data warehouse is used and how FTI is queried or targeted by end users. Parts of the system containing FTI are mapped to follow the flow of the query from a client through the authentication server to the release of the query from the database server. To use a VoIP network that provides FTI to a customer, VoIP phones must be logically protected. FTI must be encrypted while in transit within a SAN environment. SAN management traffic must also be encrypted for SAN components. To use a virtual environment that receives, processes, stores, or transmits FTI, FTI data transmitted via hypervisor management communication systems on untrusted networks must be encrypted using FIPS-approved methods provided by either the virtualization solution or third-party solution, such as a VPN that encapsulates the management traffic. To use a VoIP network that provides FTI to a customer, the VoIP traffic must be encrypted using a NIST-approved method operating in a NIST-approved mode when FTI is in transit across the network (either Internet or state agency's network). To access FTI from a web browser, the agency must encrypt FTI transmissions within the agencies internal network using a cryptographic module that is FIPS 140-2-validated.

Level HIX Implementation Requirements

Level HIX Implementation:	The information system fails securely in the event of an operational failure of a boundary protection device.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation:	The information system protects external and internal organization-defined wireless links from signal parameter attacks or references to sources for such attacks. The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system. Utilize firewalls from two [2] or more different vendors at the various levels within the network to reduce the possibility of compromising the entire network. The information systems that collectively provide name/address resolution service for the organization are fault-tolerant and implement internal/external role separation. The information system protects the confidentiality and integrity of information; any transmitted data containing sensitive information must be encrypted using a FIPS 140-2 validated module (see HHS Standard for Encryption of Computing Devices and Information). The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by approved alternative safeguards and defined in the applicable system security plan and information system risk assessment.

Level PCI Implementation Requirements	
Level PCI Implementation:	The organization ensures network diagrams identify all cardholder data connections and data flows. Using intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network, monitor all traffic at the perimeter of the cardholder data environment, as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.

Control Reference: 09.n Security of Network Services

Control Specification:	Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Documentation and Records; Monitoring; Requirements (Legal and Contractual); Services and Acquisitions; Network Security

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to Texas Health and Safety Code

Level 1 Implementation:	The ability of the network service provider to manage agreed services in a secure way is determined and regularly monitored, and the right to audit is agreed to by management. The security arrangements necessary for particular services, including security features, service levels, and management requirements, are identified and documented.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 16 CFR Part § 681.1 (e)(4) CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 CA-03 (HIGH; MOD) CMSRs v3.1 SA-09 (HIGH; MOD) CSA CCM v3.0.1 STA-03 FedRAMP CA-3 FedRAMP SA-9 IRS Pub 1075 v2016 9.3.15.7 IRS Pub 1075 v2016 9.3.4.3 ISO/IEC 27002:2013 13.1.2 ISO/IEC 27799:2016 13.1.2 MARS-E v2 CA-3 MARS-E v2 SA-9 NIST Cybersecurity Framework v1.1 DE.AE-1 NIST Cybersecurity Framework v1.1 DE.CM-6 NIST Cybersecurity Framework v1.1 ID.AM-4 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 ID.SC-1 NIST Cybersecurity Framework v1.1 PR.AT-3 NIST Cybersecurity Framework v1.1 PR.PT-4

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Texas Health and Safety Code Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The organization: 1. authorizes connections from the information system to other information systems outside of the organization through the use of interconnection security agreements or other formal agreement;

	2. centrally documents for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and 3. reviews and updates the interconnection security agreements on an ongoing basis verifying enforcement of security requirements. The organization employs, and documents in a formal agreement or other document (e.g., an applicable security plan), either (i) allow-all, deny-by-exception, or (ii) deny-all, permit-by-exception (preferred), policy for allowing specific information systems (defined in the applicable agreement, security plan, etc.) to connect to external information systems. The organization requires external/outsourced service providers to identify the specific functions, ports, and protocols used in the provision of such external/outsourced services. The contract with the external/outsourced service provider includes the specification that the service provider is responsible for the protection of covered information shared in the contract.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 16 CFR Part § 681.1 (e)(4) 21 CFR Part 11.30 CMSRs v3.1 CA-03 (HIGH; MOD) CMSRs v3.1 CA-03(05) (HIGH; MOD) CMSRs v3.1 SA-09 (HIGH; MOD) CMSRs v3.1 SA-09(02) (HIGH; MOD) FedRAMP CA-3 FedRAMP CA-3(5) FedRAMP SA-9 FFIEC IS v2016 A.6.7(a) FFIEC IS v2016 A.6.7(e) IRS Pub 1075 v2016 9.3.15.7 IRS Pub 1075 v2016 9.3.4.3 MARS-E v2 CA-3 MARS-E v2 SA-9 NIST Cybersecurity Framework v1.1 DE.AE-1 NIST Cybersecurity Framework v1.1 DE.CM-6 NIST Cybersecurity Framework v1.1 DE.CM-7 NIST Cybersecurity Framework v1.1 ID.AM-3 NIST Cybersecurity Framework v1.1 ID.AM-4 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 ID.SC-3 NIST Cybersecurity Framework v1.1 PR.AT-3 NIST Cybersecurity Framework v1.1 PR.PT-4 NIST SP 800-53 R4 CA-3b[HML]{0} NIST SP 800-53 R4 CA-3c[HML]{0} NIST SP 800-53 R4 SA-9(2)[HM]{0} NIST SP 800-53 R4 SA-9[HML]{0} NY DOH SSP v3.1 CA-3c[M]-1 NY DOH SSP v3.1 SA-9(2)[M]-0 NY DOH SSP v3.1 SA-9a[M]-1
Level Cloud Service Providers	**Implementation Requirements**
Level Cloud Service Providers Implementation:	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, are designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.
Level CMS	**Implementation Requirements**

Level CMS Implementation:	The organization records each system interconnection in the security plan for the system that is connected to the remote location. The Interconnection Security Agreement or data sharing agreement is updated following significant changes to the system, organization, or the nature of the electronic sharing of information that could impact the validity of the agreement.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The organization requires external/outsourced service providers of all external systems where Federal information is processed or stored to identify the specific functions, ports, and protocols used in the provision of the external/outsourced services. The organization prohibits the direct connection of any system processing, transmitting or storing Controlled Unclassified Information (CUI) to an external network without the use of a boundary protection device that meets Trusted Internet Connection (TIC) requirements.

Level HIX Implementation Requirements

Level HIX Implementation:	The organization records each system interconnection in the security plan for the system that is connected to the remote location and updates each interconnection security agreement following significant changes to the system, organization, or the nature of the electronic sharing of information that could impact the validity of the agreement. The organization establishes system-to-system connections with CMS through the Fed2NonFed ISA process.

Objective Name: 09.07 Media Handling

Control Objective:	Prevent unauthorized disclosure, modification, removal or destruction of information assets, or interruptions to business activities.

Control Reference: 09.o Management of Removable Media

Control Specification:	Formal procedures shall be documented and implemented for the management of removable media. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Authorization; Cryptography; Documentation and Records; Media and Assets; Physical and Facility Security; Policies and Procedures

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	

Level 1 Regulatory Factors:	Subject to CMMC Level 2 Subject to NIST 800-171 Basic Level Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Texas Health and Safety Code
Level 1 Implementation:	The organization formally establishes and enforces controls (e.g., policies and procedures) for the management of removable media and laptops including: 1. restrictions on the type(s) of media, and usages thereof, to maintain security; 2. registration of certain type(s) of media including laptops. The organization limits the use of removable media to those with a valid business need. Media containing covered and/or confidential information is physically stored, and its data encrypted in accordance with the organization's data protection and privacy policy on the use of cryptographic controls (see 06.d) until the media are destroyed or sanitized, (see 09.p) and commensurate with the confidentiality and integrity requirements for its data classification level.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 201 CMR 17.03(2)(c) 201 CMR 17.04(5) AICPA 2017 CC6.1 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMMC v1.0 MP.2.119-0 CMMC v1.0 MP.2.120-0 CMSRs v3.1 MP-01 (HIGH; MOD) CMSRs v3.1 MP-04 (HIGH; MOD) CMSRs v3.1 MP-07 (HIGH; MOD) CRR v2016 CM:G2.Q7 CSA CCM v3.0.1 EKM-03 CSA CCM v3.0.1 HRS-05 FedRAMP MP-1 FedRAMP MP-4 FedRAMP MP-7 FFIEC IS v2016 A.6.21(d) IRS Pub 1075 v2016 9.3.10.1 IRS Pub 1075 v2016 9.3.10.4 ISO/IEC 27002:2013 10.7.1 ISO/IEC 27002:2013 8.3.1 ISO/IEC 27799:2016 8.3.1 MARS-E v2 MP-1 MARS-E v2 MP-4 NIST 800-171 r2 3.8.1-0 NIST 800-171 r2 3.8.2-0 NIST Cybersecurity Framework v1.1 PR.PT-2 NIST SP 800-53 R4 MP-8[S]{1} NIST SP 800-53 R4 SA-12(9)[S]{1} NY DOH SSP v3.1 MP-2.IS.CSP3[HML]-0 NY DOH SSP v3.1 MP-4b[M]-0 NY DOH SSP v3.1 MP-7.PII1[M]-2 OCR Guidance for Unsecured PHI (1)(i) PMI DSP Framework PR.DS-1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians

	Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to CMMC Level 3 Subject to HIPAA Security Rule Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to State of Massachusetts Data Protection Act
Level 2 Implementation:	Level 1 plus: Redundancy of storage is established in light of the risks to the removable media, including where storage retention requirements exceed the rated life of the media. Organizations identify digital and non-digital media requiring restricted use and the specific safeguards necessary to restrict use. The organization: 1. protects and controls digital and non-digital media containing sensitive information during transport outside of controlled areas using cryptography and tamper-evident packaging and i. if hand carried, using a securable container (e.g., locked briefcase) via authorized personnel, or ii. if shipped, trackable with receipt by commercial carrier; 2. maintains accountability for information system media during transport outside of controlled areas; 3. documents activities associated with the transport of information system media; and 4. restricts the activities associated with transport of such media to authorized personnel.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.310(d)(1) HIPAA.SR-1 45 CFR Part § 164.310(d)(2)(iii) HIPAA.SR-1 CMMC v1.0 MP.3.124-1 CMSRs v3.1 MP-05 (HIGH; MOD) CMSRs v3.1 MP-05(04) (HIGH; MOD) CMSRs v3.1 MP-07 (HIGH; MOD) CRR v2016 CM:G2.Q7 FedRAMP MP-5 FedRAMP MP-5(4) FedRAMP MP-7 IRS Pub 1075 v2016 9.3.10.5 ISO/IEC 27002:2013 8.3.1 ISO/IEC 27799:2016 8.3.1 MARS-E v2 MP-5 MARS-E v2 MP-5(4) NIST 800-171 r2 3.8.5-1 NIST Cybersecurity Framework v1.1 PR.PT-2 NRS 603A.215.1 NY DOH SSP v3.1 MP-7[M]-2 PCI DSS v3.2.1 9.6.3

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients

	IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 2 Subject to CMMC Level 3 Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: Organizations restrict the use of writable, removable media and personally-owned, removable media in organizational systems.
Level 3 Control Standard Mapping:	CMMC v1.0 MP.2.121-0 CMMC v1.0 MP.3.123-2 CMSRs v3.1 MP-06(03) (HIGH) CMSRs v3.1 MP-07(01) (HIGH; MOD) CRR v2016 CM:G2.Q7 FedRAMP MP-7(1) ISO/IEC 27002:2013 8.3.1 ISO/IEC 27799:2016 8.3.1 NIST 800-171 r2 3.8.7-0 NIST 800-171 r2 3.8.8-2 NIST Cybersecurity Framework v1.1 PR.PT-2 NIST SP 800-53 R4 MP-2[HML]{0} NIST SP 800-53 R4 MP-7[HML]{0} NY DOH SSP v3.1 MP-2a[HML]-1 NY DOH SSP v3.1 MP-7[M]-1

Level CIS Implementation Requirements

Level CIS Implementation:	The organization limits the use of removable media to those with a valid business need. If such devices are required, the organization: 1. configures systems to allow only specific USB devices (based on serial number or other unique property) to be accessed; and 2. automatically configures devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected, e.g., through the use of third-party software.

Level CMS Implementation Requirements

Level CMS Implementation:	The organization physically controls and securely stores digital and non-digital media defined within NIST SP 800-88, Guidelines for Media Sanitization, within controlled

	areas using physical security safeguards prescribed for the highest system security level of the information ever recorded on it. If PII is recorded on magnetic media with other data, it is protected as if it were entirely personally identifiable information. Portable, removable storage devices are sanitized prior to connecting such devices to the information system under the following circumstances: 1. initial use after purchase; 2. when obtained from an unknown source; 3. when the organization loses a positive chain of custody; and 4. when the device was connected to a lower assurance system based on its security categorization (e.g., a publicly accessible kiosk).

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

Control Reference: 09.p Disposal of Media

Control Specification:	Media shall be disposed of securely and safely when no longer required, using formal procedures that are documented. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Media and Assets; Policies and Procedures; Services and Acquisitions; Third-parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to HIPAA Security Rule Subject to Joint Commission Accreditation Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to Supplemental Requirements Subject to Texas Health and Safety Code
Level 1 Implementation:	The organization destroys media when it is no longer needed for business or legal reasons. Formal procedures for the secure disposal of media minimize the risk of information leakage to unauthorized persons. The procedures for the secure disposal of media containing information are commensurate with the sensitivity of that information. The following items are addressed:

	1. the use of generally-accepted secure disposal or erasure methods (see 08.l) for use by another application within the organization, for media that contains (or might contain) covered and/or confidential information; and 2. the identification of information that qualifies as covered, or a policy is developed that all information is considered covered and/or confidential in the absence of unequivocal evidence to the contrary. It may be easier to arrange for all media items to be collected and disposed of securely, rather than attempting to separate out the items containing covered and/or confidential information. If collection and disposal services offered by other organizations are used, care is taken in selecting a suitable contractor with adequate controls and experience.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.310(d)(2)(i) HIPAA.SR-1 45 CFR Part § 164.310(d)(2)(i) HIPAA.SR-3 AICPA 2017 CC6.5 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 DM-02 (HIGH; MOD) CMSRs v3.1 MP-06 (HIGH; MOD) CRR v2016 AM:G6.Q6 CRR v2016 AM:G6.Q7 CRR v2016 CM:G2.Q5 CSA CCM v3.0.1 DSI-07 FedRAMP MP-6 FFIEC IS v2016 A.6.18(e) IRS Pub 1075 v2016 9.3.10.6 IRS Pub 1075 v2016 9.4.18 IRS Pub 1075 v2016 9.4.8 IRS Pub 1075 v2016 9.4.9 IRS Pub 1075 v2016 Exhibit 10 ISO/IEC 27002:2013 8.3.2 ISO/IEC 27799:2016 8.3.2 MARS-E v2 DM-2 MARS-E v2 MP-6 NIST Cybersecurity Framework v1.1 PR.DS-3 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.IP-6 NIST SP 800-53 R4 MP-8[S]{2} NRS 603A.215.1 NY DOH SSP v3.1 MP-6b[M]-1 OCR Guidance for Unsecured PHI (2)(i) OCR Guidance for Unsecured PHI (2)(ii) PCI DSS v3.2.1 9.8 SR v6.4 17.7-0 TJC IM.02.01.03, EP 3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance

	Subject to MARS-E Requirements Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: Procedures are implemented to prevent the aggregation effect, which may cause a large quantity of non-covered information to become covered when accumulating media for disposal.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 MP-06(01) (HIGH) CMSRs v3.1 MP-06(02) (HIGH) IRS Pub 1075 v2016 9.4.7 ISO/IEC 27002:2013 8.3.2 ISO/IEC 27799:2016 8.3.2 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.IP-6

Level CMS Implementation Requirements

Level CMS Implementation:	The organization reviews, approves, tracks, documents (logs), and verifies media sanitization and disposal actions. The organization tests sanitization equipment and procedures within every 365 days to verify that the intended sanitization is being achieved.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The organization tests sanitization equipment and procedures within every 365 days to verify that the intended sanitization is being achieved.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	The agency cleanses FTI at the staging area of a data warehouse and documents how it cleanses the FTI when it is extracted, transformed, and loaded (i.e., in the ETL process). In addition, the agency describes the process of object reuse once FTI is replaced from data sets. All FTI must be removed from media in the data warehouse by a random overwrite software program. If the media will be reused by the agency for the same purpose of storing FTI and will not be leaving organization control, then clearing is a sufficient method of sanitization. If the media will be reused and repurposed for a non-FTI function or will be leaving organization control (i.e., media being exchanged for warranty, cost rebate, or other purposes - and where the specific media will not be returned to the agency), then purging is selected as the sanitization method. If the media will not be reused at all, then destroying is the method for media sanitization. The following media sanitization requirements are applicable for media used in 'pre-production' or 'test' environments: 1. The technique for clearing, purging, and destroying media depends on the type of media being sanitized. 2. A representative sampling of media must be tested after sanitization has been completed; and 3. Media sanitization is witnessed or verified by an agency employee.

	Disposal of all Multifunction Device (MFD) hardware (e.g., hard disks) and WLAN components follows the organization's standard media sanitization and disposal procedure requirements. FTI furnished to the user and any paper material generated therefrom, such as extra copies, photo impressions, computer printouts, carbon paper, notes, stenographic notes, and work papers must be destroyed by burning, mulching, pulping, shredding, or disintegrating. FTI must never be disclosed to an agency's agents or contractors during disposal, unless authorized by the Internal Revenue Code. Agencies must review and approve media to be sanitized to ensure compliance with records-retention policies. Tracking/documenting actions include, for example, listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, specific files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken, personnel who performed the verification, and disposal action taken. Agencies verify that the sanitization of the media was effective prior to disposal.

Level HIX Implementation Requirements

Level HIX Implementation:	The organization reviews, approves, tracks, documents (logs), and verifies media sanitization and disposal actions. The organization tests sanitization equipment and procedures within every 365 days to verify that the intended sanitization is being achieved.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The organization finely shreds, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and procedures.

Control Reference: 09.q Information Handling Procedures

Control Specification:	Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Cryptography; Data Loss Prevention; Documentation and Records; Media and Assets; Monitoring; User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 3 Subject to IRS Pub 1075 Compliance Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High)

	Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to State of Massachusetts Data Protection Act
Level 1 Implementation:	Procedures for handling, processing, communication and storage of information (including information media awaiting disposal) are established, monitored, and enforced to protect data from unauthorized disclosure or misuse including: 1. physical and technical access restrictions commensurate with the data classification level; 2. handling and labeling of all media according to its indicated classification (sensitivity) level; 3. periodic review (at a minimum annually) of distribution and authorized recipient lists; and 4. monitoring the status and location of media containing unencrypted covered information.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(ii) 1 TAC § 390.2(a)(4)(A)(xi) 201 CMR 17.03(2)(c) 201 CMR 17.03(2)(g) CMMC v1.0 MP.3.122-0 CMSRs v3.1 MP-03 (HIGH; MOD) CMSRs v3.1 SI-12 (HIGH; MOD) CRR v2016 AM:G6.Q3 CRR v2016 AM:G6.Q7 FedRAMP MP-2 FedRAMP MP-3 FedRAMP SI-12 IRS Pub 1075 v2016 4.5 IRS Pub 1075 v2016 9.3.10.2 IRS Pub 1075 v2016 9.3.10.3 IRS Pub 1075 v2016 9.3.17.9 ISO/IEC 27002:2013 8.2.3 ISO/IEC 27799:2016 8.2.3 MARS-E v2 MP-2 MARS-E v2 MP-3 MARS-E v2 SI-12 NIST 800-171 r2 3.8.4-0 NIST Cybersecurity Framework v1.1 PR.DS-3 NIST Cybersecurity Framework v1.1 PR.PT-2 NIST SP 800-53 R4 AC-16b[S]{2} NIST SP 800-53 R4 MP-3[HM]{0} NRS 603A.215.1 NY DOH SSP v3.1 MP-3a[M]-0 PCI DSS v3.2.1 9.5

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to FISMA Compliance Subject to PCI Compliance

Level 2 Implementation:	Level 1 plus: The organization maintains inventories of media to maintain strict control over storage and accessibility. Management approves any and all media that is moved from a secured area, especially when media is distributed to individuals. Maintenance of formal records of data transfers, including logging and an audit trail, is maintained.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 MP-02 (HIGH; MOD) CMSRs v3.1 MP-05 (HIGH; MOD) FedRAMP MP-2 FedRAMP MP-5 IRS Pub 1075 v2016 4.5 IRS Pub 1075 v2016 9.3.10.2 IRS Pub 1075 v2016 9.3.10.5 ISO/IEC 27002:2013 8.2.3 ISO/IEC 27799:2016 8.2.3 MARS-E v2 MP-2 MARS-E v2 MP-5 NIST Cybersecurity Framework v1.1 PR.DS-3 NIST Cybersecurity Framework v1.1 PR.PT-2 NRS 603A.215.1 PCI DSS v3.2.1 3.2 PCI DSS v3.2.1 3.2.1 PCI DSS v3.2.1 3.2.2 PCI DSS v3.2.1 3.2.3 PCI DSS v3.2.1 9.6 PCI DSS v3.2.1 9.6.3 PCI DSS v3.2.1 9.7

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to CMMC Level 3 Subject to FedRAMP Certification Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: Inventory and disposition records for information system media are maintained to ensure control and accountability of the organization's information. The media related records contain sufficient information to reconstruct the data in the event of a breach. The media records, at a minimum, contain: 1. the name of media recipient;

	2. the signature of media recipient; 3. the date/time media received; 4. the media control number and contents; 5. the movement or routing information; and 6. if disposed of, the date, time, and method of destruction. The information system implements cryptographic mechanisms to protect the confidentiality and integrity of sensitive (non-public) information stored on digital media during transport outside of controlled areas.
Level 3 Control Standard Mapping:	CMMC v1.0 MP.3.125-0 CMSRs v3.1 MP-05(04) (HIGH; MOD) CMSRs v3.1 MP-CMS-1 (HIGH; MOD) FedRAMP MP-5 FedRAMP MP-5(4) MARS-E v2 MP-5(4) MARS-E v2 MP-CMS-1 NIST 800-171 r2 3.8.6-0 NIST Cybersecurity Framework v1.1 PR.DS-3 NIST SP 800-53 R4 MP-5(4)[HM]{0} NY DOH SSP v3.1 MA-4(6)[MN]-2 NY DOH SSP v3.1 MP-5(4)[M]-0

Level HIX Implementation Requirements

Level HIX Implementation:	The organization employs automated mechanisms to (ii) restrict access to sensitive information (e.g., PII) residing on digital and non-digital media to authorized individuals; and (ii) restricts access to media storage areas, to audit access attempts and access granted. Inventory and disposition records for information system media are maintained to ensure control and accountability of CMS information. The media-related records contain sufficient information to reconstruct the data in the event of a breach.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	Commensurate with the FIPS 199 security categorizations for confidentiality and integrity of the data, the organization (i) protects and controls digital and non-digital media defined within the latest revision of NIST SP 800-88, Guidelines for Media Sanitization, and HHS Information Systems Security and Privacy Policy (IS2P) Appendix I, containing sensitive information during transport outside of controlled areas using cryptography and tamper evident packaging, and: (a) if hand carried, using a securable container (e.g., locked briefcase) via authorized personnel; or (b) if shipped, trackable with receipt by commercial carrier; (ii) maintains accountability for information system media during transport outside of controlled areas; (iii) documents activities associated with the transport of information system media; and (iv) restricts the activities associated with the transport of information system media to authorized personnel. CSPs define security measures to protect digital and non-digital media in transport. The security measures are approved and accepted by the Joint Authorization Board (JAB). The information system media records, at a minimum, contain (i) the name of media recipient; (ii) signature of media recipient; (iii) date/time media received; (iv) media control number and contents; (v) movement or routing information; and (vi) if disposed of, the date, time, and method of destruction.

Level PCI Implementation Requirements

Level PCI Implementation:	The system does not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, the system renders all data unrecoverable upon completion of the authorization process. The system does not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data. The system does not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization. The system does not store the personal identification number (PIN) or the encrypted PIN block after authorization. The system masks the PAN when displaced (the first six or last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN. (Note this requirement does not supersede stricter requirements in place for displays of cardholder data (for example, legal or payment card brand requirements for point-of-sale (POS) receipts).

Control Reference: 09.r Security of System Documentation

Control Specification:	System documentation shall be protected against unauthorized access.
Factor Type:	Organizational
Topics:	Authorization; Documentation and Records; User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	The organization: 1. Obtains administrator documentation for the information system, system component, or information system service that describes: i. Secure configuration, installation, and operation of the system, component, or service; ii. Effective use and maintenance of security functions/mechanisms; and iii. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; 2. Obtains user documentation for the information system, system component, or information system service that describes:

	i. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; ii. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and iii. User responsibilities in maintaining the security of the system, component, or service. Organizations documents attempts to obtain information system documentation when such documentation is either unavailable or non-existent. The organization protects system documentation in accordance with the organization's risk management strategy, e.g., by access controls (see 1.0), and distributes documentation to organization-defined personnel with the need for such documentation. The access list for system documentation is kept to a minimum and authorized by the application owner.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 SA-05 (HIGH; MOD) CSA CCM v3.0.1 BCR-04 FedRAMP SA-5 IRS Pub 1075 v2016 9.3.15.5 MARS-E v2 SA-5 NIST Cybersecurity Framework v1.1 ID.RA-1 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST SP 800-53 R4 SA-5c[HML]{0} NIST SP 800-53 R4 SA-5d[HML]{0} NIST SP 800-53 R4 SA-5e[HML]{0} NY DOH SSP v3.1 SA-5c[M]-0 NY DOH SSP v3.1 SA-5d[M]-0 NY DOH SSP v3.1 SA-5e[M]-0

Objective Name: 09.08 Exchange of Information

Control Objective:	Ensure the exchange of information within an organization and with any external entity is secured and protected and carried out in compliance with relevant legislation and exchange agreements.

Control Reference: 09.s Information Exchange Policies and Procedures

Control Specification:	Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication mediums. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Awareness and Training; Communications and Transmissions; Cryptography; Personnel; Policies and Procedures; Third-parties and Contractors; Viruses and Malware

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 3 Subject to FISMA Compliance Subject to HIPAA Security Rule

	Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Supplemental Requirements
Level 1 Implementation:	The organization ensures that communications protection requirements, including the security of exchanges of information, is the subject of policy development (see also 04.a and 04.b) and compliance audits (see 06.g) consistent with relevant legislation. When using electronic communication applications or systems for information exchange, the following items are addressed: 1. policies or guidelines are defined outlining acceptable use of electronic communication applications or systems; 2. the use of anti-malware for the detection of and protection against malicious code that may be transmitted through the use of electronic communications; 3. procedures are implemented for the use of wireless communications including an appropriate level of encryption (see 09.m); 4. employee, contractor and any other user's responsibilities are defined to not compromise the organization (e.g., through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.); 5. the required use of cryptographic techniques to protect the confidentiality, integrity and authenticity of covered information; 6. the retention and disposal guidelines are defined for all business correspondence, including messages, in accordance with relevant national and local legislation and regulations; and 7. controls and restrictions are implemented associated with the forwarding of communications (e.g., automatic forwarding of electronic mail to external mail addresses). The organization establishes terms and conditions, consistent with any trust relationship established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: 1. access the information system from external information systems; and 2. process, store, or transmit organization-controlled information using external information systems. Personnel are appropriately educated and periodically reminded of the following: 1. not to leave covered or critical information on printing systems (e.g., copiers, printers, and facsimile machines) as these may be accessed by unauthorized personnel; 2. that they take necessary precautions, including not to reveal covered information, to avoid being overheard or intercepted when making a phone call by: i. people in their immediate vicinity - particularly when using mobile phones, ii. wiretapping, and other forms of eavesdropping through physical access to the phone handset or the phone line, or using scanning receivers, or iii. people at the recipient's end; 3. not leaving messages containing sensitive information on answering machines since these may be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialing; 4. the problems of using facsimile machines, namely: i. unauthorized access to built-in message stores to retrieve messages,

	ii. deliberate or accidental programming of machines to send messages to specific numbers, and iii. sending documents and messages to the wrong number either by misdialing or using the wrong stored number; 5. not to register demographic data, such as the email address or other personal information, in any software to avoid collection for unauthorized use; and 6. that modern facsimile machines and photocopiers have page caches and store pages in case of a paper or transmission fault, which will be printed once the fault is cleared. Cryptography is used to protect the confidentiality and integrity of remote access sessions to the internal network and to external systems. Formal procedures are defined to encrypt data in transit including use of strong cryptography protocols to safeguard covered information during transmission over less trusted/open public networks. Valid encryption processes include: 1. Transport Layer Security (TLS) 1.2 or later; 2. IPSec VPNs: i. Gateway-To-Gateway Architecture, ii. Host-To-Gateway Architecture, or iii. Host-To-Host Architecture; 3. TLS VPNs: i. Portal VPN, or ii. Tunnel VPN See NIST SP 800-52 Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementation and NIST SP 800-77 Guide to IPsec VPNs for more information on implementing encryption technologies for information transmissions. Examples of less trusted/open, public networks include: 1. the Internet; 2. wireless technologies; 3. Global System for Mobile communications (GSM); and 4. General Packet Radio Service (GPRS).
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.312(e)(1) HIPAA.SR-2 AICPA 2017 CC6.7 CMMC v1.0 AC.3.014-0 CMSRs v3.1 AC-17 (HIGH; MOD) CMSRs v3.1 AC-17(02) (HIGH; MOD) CMSRs v3.1 AC-20 (HIGH; MOD) CMSRs v3.1 SC-01 (HIGH; MOD) CRR v2016 CM:G2.Q4 CSA CCM v3.0.1 AIS-04 FedRAMP AC-17 FedRAMP AC-17(2) FedRAMP AC-19(5) FedRAMP AC-20 FedRAMP SC-1 FFIEC IS v2016 A.6.23 FFIEC IS v2016 A.6.24 IRS Pub 1075 v2016 4.7.3 IRS Pub 1075 v2016 9.3.1.12 IRS Pub 1075 v2016 9.3.1.15 IRS Pub 1075 v2016 9.3.16.1 ISO/IEC 27002:2013 13.2.1 ISO/IEC 27799:2016 13.2.1 MARS-E v2 AC-17 MARS-E v2 AC-17(2) MARS-E v2 AC-20 MARS-E v2 SC-1

	NIST 800-171 r2 3.1.13-0 NIST Cybersecurity Framework v1.1 PR.AT-1 NIST SP 800-53 R4 AC-18a[HML]{0} NIST SP 800-53 R4 AC-20[HML]{0} NIST SP 800-53 R4 IA-9(1)[S]{1} NIST SP 800-53 R4 MA-4(4)b[S]{2} NIST SP 800-53 R4 MA-4(6)[S]{0} NIST SP 800-53 R4 SA-9(3)[S]{0} NIST SP 800-53 R4 SC-43[S]{0} NY DOH SSP v3.1 AC-17(2)[M]-0 NY DOH SSP v3.1 AC-17.IS3e[M]-1 NY DOH SSP v3.1 MA-4(6)[MN]-1 PCI DSS v3.2.1 2.3 PCI DSS v3.2.1 4.1 PCI DSS v3.2.1 4.1.1 PMI DSP Framework PR.DS-1 SR v6.4 45-0 TJC IM.02.01.03, EP 1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to CMMC Level 2 Subject to FedRAMP Certification Subject to IRS Pub 1075 Compliance Subject to Joint Commission Accreditation Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to State of Massachusetts Data Protection Act Subject to the CMS Minimum Security Requirements (High) Subject to the State of Nevada Security of Personal Information Requirements
Level 2 Implementation:	Level 1 plus: The organization permits authorized individuals to use an external information system to access the information system or to process, store or transmit organization-controlled information only when the organization: 1. verifies the implementation of required security controls on the external system, as specified in the organization's information security policy and security plan; or 2. retains approved information connection or processing agreements with the organizational entity hosting the external information system (see 09.t). The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.

	Terms and conditions are established for authorized individuals to: 1. access the information system from an external information system; and 2. process, store and/or transmit organization-controlled information using an external information system. The information system: 1. prohibits remote activation of collaborative computing devices; and 2. provides an explicit indication of use to users physically present at the devices.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 201 CMR 17.04(3) CAQH Core Phase 1 153: Eligibility and Benefits Connectivity Rule v1.1.0 Subsection 5.2 CMMC v1.0 AC.2.006-0 CMMC v1.0 SC.2.178-0 CMSRs v3.1 AC-20 (HIGH; MOD) CMSRs v3.1 AC-20(01) (HIGH; MOD) CMSRs v3.1 AC-20(02) (HIGH; MOD) CMSRs v3.1 SC-15 (HIGH; MOD) CMSRs v3.1 SC-15(01) (HIGH; MOD) COBIT 5 DS5.11 COBIT 5 DSS05.02 CSA CCM v3.0.1 EKM-03 FedRAMP AC-20 FedRAMP AC-20(1) FedRAMP AC-20(2) FedRAMP SC-15 IRS Pub 1075 v2016 9.3.1.15 IRS Pub 1075 v2016 9.3.16.10 IRS Pub 1075 v2016 9.4.9 MARS-E v2 AC-20 MARS-E v2 AC-20(1) MARS-E v2 AC-20(2) MARS-E v2 AR-4 MARS-E v2 SC-15 MARS-E v2 SC-15(1) NIST 800-171 r2 3.1.21-0 NIST 800-171 r2 3.13.12-0 NIST Cybersecurity Framework v1.1 PR.AC-3 NIST SP 800-53 R4 AC-20(1)[HM]{0} NIST SP 800-53 R4 AC-20(2)[HM]{0} NIST SP 800-53 R4 SC-15a[HML]{0} NIST SP 800-53 R4 SC-15b[HML]{0} NRS 603A.215.1 NRS 603A.215.2.a NY DOH SSP v3.1 AC-20(2)[M]-0 NY DOH SSP v3.1 SC-15a[M]-0 NY DOH SSP v3.1 SC-15b[M]-0 OCR Guidance for Unsecured PHI (1)(ii) TJC IM.02.01.03, EP 5
Level Cloud Service Providers	**Implementation Requirements**
Level Cloud Service Providers Implementation:	Cloud service providers use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service and make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved. The provider uses an industry-recognized virtualization platform and standard virtualization formats (e.g., Open Virtualization Format, OVF) to help ensure interoperability, and has documented custom changes made to any hypervisor in use and all solution-specific virtualization hooks available for customer review.
Level CMS	**Implementation Requirements**

Level CMS Implementation:	The organization prohibits the use of external information systems, including, but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports, to store, access, transmit, or process CMS sensitive information, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If external information systems are authorized, the organization establishes strict terms and conditions for their use. The terms and conditions address, at a minimum: 1. the types of applications that can be accessed from external information systems; 2. the maximum FIPS 199 security category of information that can be processed, stored, and transmitted; 3. how other users of the external information system will be prevented from accessing federal information; 4. the use of virtual private networking (VPN) and firewall technologies; 5. the use of and protection against the vulnerabilities of wireless technologies; 6. the maintenance of adequate physical security controls; 7. the use of virus and spyware protection software; and 8. how often the security capabilities of installed software are to be updated. The organization prohibits running collaborative computing mechanisms, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the authorization specifically identifies allowed mechanisms, allowed purpose(s), and the information system upon which the mechanisms can be used.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	Unless approved by the Office of Safeguards, the agency must prohibit: 1. Access to FTI from external information systems; 2. Use of agency-controlled portable storage devices (e.g., flash drives, external hard drives) containing FTI on external information systems; and 3. Use of non-agency-owned information systems; system components; or devices to process, store, or transmit FTI. Any non-agency-owned information system usage requires the agency to notify the Office of Safeguards 45 days prior to implementation. All FTI data in transit to and from a Multifunctional Device (MFD) is encrypted when moving across a WAN and within the LAN.

Level GDPR Implementation Requirements

Level GDPR Implementation:	The organization maintains records of the basis used to authorize cross-border flows of personal data to a third country or international organization, which include but are not limited to: 1. an adequacy decision by the EU Commission; 2. the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available; 3. binding corporate rules approved by the relevant supervisory authority; 4. A court judgement or administrative decision of a third country if based on an international agreement between the third country and the EU; or 5. If one of the following conditions are met:

i. the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards,
ii. the transfer is necessary for the performance of a contract between the data subject and the controller, or the implementation of pre-contractual measures taken at the data subject's request,
iii. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person,
iv. the transfer is necessary for important reasons of public interest,
v. the transfer is necessary for the establishment, exercise or defense of legal claims,
vi. the transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent,
vii. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in EU or Member State law for consultation are fulfilled in the particular case.

Appropriate safeguards include:

1. a legally binding and enforceable instrument between public authorities or bodies;
2. binding corporate rules;
3. standard data protection clauses adopted by the Commission;
4. standard data protection clauses adopted by a supervisory authority and approved by the Commission;
5. an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
6. an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

If authorized by the relevant supervisory authority, appropriate safeguards may also include:

1. contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organization; or
2. provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

Level HIX Implementation Requirements

Level HIX Implementation:	The organization prohibits the use of external information systems—including, but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports—by organizational users (staff and contractors within the organization) to store, access, transmit, or process sensitive information (such as FTI or Privacy Act protected information), unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization establishes strict terms and conditions for their use. For non-organizational users (such as business partners), the Administering Entity organization establishes terms and conditions, consistent with CMS implementation

	guidance of HHS Regulation 45 C.F.R. § 115.260, and in compliance with legal data sharing agreements signed with CMS, for any trust relationships established with other organizations owning, operating, and/or maintaining external information systems. These terms and conditions allow authorized individuals to: 1. Access the information system from external information systems; and 2. Process, store, or transmit organization-controlled information using external information systems.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The information system does not release information outside of the established system boundary unless: (i) the receiving external organization (i.e., department, agency, or commercial entity not managed by CMS) provides information security and privacy safeguards commensurate with those implemented by CMS; and (ii) CMS-defined information security and privacy safeguards are used to validate the appropriateness of the information designated for release. For systems processing, storing, or transmitting PII (to include PHI), the information system does not release information outside of the established system boundary unless (i) the receiving organization or information system provides privacy and security controls commensurate with the PII confidentiality impact level of the PII being received; and (ii) controls UL-1 and UL-2 are used to validate the appropriateness of the information designated for release. Executive management is responsible for communicating requirements of this policy (NYS-P03-002 Information Security Policy) and the associated standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third-party agreements. For non-public information to be released outside the organization or shared between state entities, a process must be established that, at a minimum: (i) evaluates and documents the sensitivity of the information to be released or shared; (ii) identifies the responsibilities of each party for protecting the information; (iii) defines the minimum controls required to transmit and use the information; (iv) records the measures that each party has in place to protect the information; (v) defines a method for compliance measurement; (vi) provides a signoff procedure for each party to accept responsibilities; and (vii) establishes a schedule and procedure for reviewing the controls. The CMS CIO, CISO, and SOP have the authority to order the immediate termination and/or suspension of any interconnection that, in the judgment of the CMS officer and CMS Security Operations, present an unacceptable level of risk to the CMS enterprise and/or mission. All publicly accessible federal websites and web services shall employ secure connections, such as HTTPS. Transport Layer Security (TLS) shall be implemented and configured in accordance with the recommendation of NIST SP 800-52, as amended. Websites and services shall deploy HTTPS in a manner that allows for rapid updates to certificates, cipher choices protocol versions, and other configuration elements. Websites and services available over HTTPS shall enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS going forward. Allowing HTTP connections for the sole purpose of redirecting clients to HTTPS connections shall be acceptable and encouraged; HSTS headers must specify a max-age of at least one [1] year.

Control Reference: 09.t Exchange Agreements

Control Specification:	Agreements shall be established and implemented for the exchange of information and software between the organization and external parties.
Factor Type:	Organizational
Topics:	Communications and Transmissions; Data Loss Prevention; IT Organization and Management Roles and Responsibilities; Media and Assets; Requirements (Legal and Contractual); Third-parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to HITRUST De-ID Framework Requirements Subject to Texas Health and Safety Code Subject to the State of Nevada Security of Personal Information Requirements
Level 1 Implementation:	Exchange and data sharing agreements specify the minimum set of controls on responsibility, procedures, technical standards and solutions. The exchange agreements also specify organization policies including: 1. classification policy for the sensitivity of the business information; 2. management responsibilities for controlling and notifying transmission, dispatch, and receipt; 3. procedures for notifying sender of transmission, dispatch, and receipt; 4. procedures to ensure traceability and non-repudiation; 5. minimum technical standards for packaging and transmission; 6. courier identification standards; 7. responsibilities and liabilities in the event of information security incidents, such as loss of data; 8. use of an agreed labeling system for covered or critical information, ensuring that the meaning of the labels is immediately understood, and that the information is appropriately protected; 9. ownership and responsibilities for data protection, copyright, software license compliance and similar considerations; 10. technical standards for recording and reading information and software; 11. any special controls that may be required to protect covered items, including cryptographic keys; and 12. escrow agreements. Policies, procedures, and standards are established and maintained to protect information and physical media in transit and are referenced in such exchange agreements.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 201 CMR 17.03(2)(c) CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 MP-01 (HIGH; MOD) COBIT 5 DS5.11 COBIT 5 DSS05.02 CSA CCM v3.0.1 STA-05 De-ID Framework v1 Data Sharing Agreements: DSAs FedRAMP MP-1

	IRS Pub 1075 v2016 9.3.10.1 ISO/IEC 27002:2013 13.2.2 ISO/IEC 27799:2016 13.2.2 MARS-E v2 MP-1 NIST Cybersecurity Framework v1.1 PR.AT-3 NIST Cybersecurity Framework v1.1 PR.DS-2 NIST Cybersecurity Framework v1.1 PR.PT-2

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	If the interconnecting systems have the same AO (or same primary operational IT infrastructure manager), an interconnection agreement document is not required; rather, the interface characteristics between the interconnecting information systems are described in the security plans for the respective systems. Systems processing, storing, or transmitting PHI: When acquiring information systems, components, or services used to store, process, or transmit PHI, in addition to the requirements for PII, ensure, in consultation with the privacy office, that any necessary memorandum of understanding, memorandum of agreement, and other data sharing agreement are obtained.

Control Reference: 09.u Physical Media in Transit

Control Specification:	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond the organization's physical boundaries.
Factor Type:	Organizational
Topics:	Communications and Transmissions; Cryptography; Media and Assets; Policies and Procedures; Services and Acquisitions

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to PCI Compliance Subject to Texas Health and Safety Code
Level 1 Implementation:	The following procedures are established to protect information media being transported between sites: 1. reliable transport or couriers that can be tracked are used; 2. a list of authorized couriers is agreed upon with management; 3. procedures to check the identification of couriers are developed; and 4. packaging is sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications (e.g., for software) for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture, or electromagnetic fields. Controls are adopted to protect covered information from unauthorized disclosure or modification, including at least one of the following: 1. use of locked containers; 2. delivery by hand; 3. tamper-evident packaging (which reveals any attempt to gain access); or

	4. splitting of the consignment into more than one delivery, and dispatch by different routes.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 MP-05 (HIGH; MOD) CSA CCM v3.0.1 HRS-05 FFIEC IS v2016 A.6.18(f) IRS Pub 1075 v2016 9.3.10.5 ISO/IEC 27002:2013 8.3.3 ISO/IEC 27799:2016 8.3.3 MARS-E v2 MP-5 NIST Cybersecurity Framework v1.1 PR.DS-2 NIST Cybersecurity Framework v1.1 PR.PT-2 NRS 603A.215.1 PCI DSS v3.2.1 9.6.2

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to Joint Commission Accreditation Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (Supplemental) Subject to the CMS Minimum Security Requirements (High) Subject to the EU GDPR Subject to the State of Nevada Security of Personal Information Requirements
Level 2 Implementation:	Level 1 plus: Media is encrypted when being moved off site. Media is encrypted onsite unless physical security can be guaranteed. The information system implements cryptographic mechanisms to protect the confidentiality and integrity of sensitive (non-public) information stored on digital media during transport outside of control areas.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 MP-05 (HIGH; MOD) CMSRs v3.1 MP-05(04) (HIGH; MOD) CMSRs v3.1 PE-16 (HIGH; MOD) CMSRs v3.1 SC-28 (HIGH; MOD) COBIT 5 DS5.11 COBIT 5 DSS05.02 FedRAMP MP-5 FedRAMP MP-5(4) FedRAMP PE-16 FedRAMP SC-28

	FFIEC IS v2016 A.6.18(f) IRS Pub 1075 v2016 4.3.1 IRS Pub 1075 v2016 4.4 IRS Pub 1075 v2016 9.3.10.5 IRS Pub 1075 v2016 9.3.11.8 IRS Pub 1075 v2016 9.3.16.15 ISO/IEC 27002:2013 8.3.3 ISO/IEC 27799:2016 8.3.3 MARS-E v2 MP-5 MARS-E v2 MP-5(4) MARS-E v2 PE-16 MARS-E v2 SC-28 NIST Cybersecurity Framework v1.1 PR.DS-2 NIST Cybersecurity Framework v1.1 PR.PT-2 NIST SP 800-53 R4 SC-34(2)[S]{0} NRS 603A.215.2.a NRS 603A.215.2.b PCI DSS v3.2.1 9.5 PCI DSS v3.2.1 9.6 TJC IM.02.01.03, EP 5

Level CMS Implementation Requirements

Level CMS Implementation:	The organization: 1. protects and controls digital and non-digital media containing CMS sensitive information during transport outside of controlled areas using cryptography and tamper-evident packaging, and i. if hand-carried, using securable container (e.g., locked briefcase) via authorized personnel, or ii. if shipped, trackable with receipt by commercial carrier; 2. maintains accountability for information system media during transport outside of controlled areas; and 3. restricts the activities associated with transport of such media to authorized personnel.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	All transportation or shipments of FTI (including electronic media or microfilm) must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged. All FTI transported through the mail or courier/messenger service must be double-sealed; that is one envelope within another envelope. The inner envelope is marked confidential with some indication that only the designated official or delegate is authorized to open it.

Control Reference: 09.v Electronic Messaging

Control Specification:	Information involved in electronic messaging shall be appropriately protected. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Authentication; Authorization; Communications and Transmissions

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	

Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to HIPAA Security Rule Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	Legal considerations, including requirements for electronic signatures, are addressed. Approval is obtained prior to using external public services, including instant messaging or file sharing. Stronger levels of authentication controlling access from publicly accessible networks are implemented. Stronger controls, such as electronic signatures, are implemented to protect certain electronic messages (e.g., those containing PII or other covered information). The electronic messages are protected throughout the duration of its end-to-end transport path. Cryptographic mechanisms are employed to protect message integrity and confidentiality unless protected by alternative measures, e.g., physical controls. The organization never sends unencrypted sensitive information (e.g., covered information, PANs, FTI) by end-user messaging technologies (e.g., email, instant messaging, and chat).
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 201 CMR 17.04(3) 45 CFR Part § 164.312(e)(2)(i) HIPAA.SR-2 CMSRs v3.1 SC-08 (HIGH; MOD) CMSRs v3.1 SC-08(01) (HIGH; MOD) CMSRs v3.1 SC-CMS-1 (HIGH; MOD) COBIT 5 DS5.11 COBIT 5 DSS05.02 CRR v2016 CM:G2.Q4 FedRAMP SC-8 IRS Pub 1075 v2016 9.3.16.6 IRS Pub 1075 v2016 9.4.3 IRS Pub 1075 v2016 9.4.4 ISO/IEC 27002:2013 13.2.3 ISO/IEC 27799:2016 13.2.3 MARS-E v2 SC-8 MARS-E v2 SC-8(1) MARS-E v2 SC-8(2) MARS-E v2 SC-ACA-1 MARS-E v2 SC-ACA-2 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 PR.DS-2 NIST Cybersecurity Framework v1.1 PR.DS-5 NRS 603A.215.2.a NY DOH SSP v3.1 SC-CMS-1[M]-2 PCI DSS v3.2.1 4.2

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	If FTI is allowed to be included within emails or email attachments, the agency must only transmit FTI to an authorized recipient. Encrypt email transmissions that contain FTI using a FIPS 140-2 validated mechanism. If FTI is allowed to be included within fax communications, the agency must only transmit FTI to an authorized recipient and must adhere to the following requirements: 1. Have a trusted staff member at both the sending and receiving fax machines; and 2. Accurately maintain broadcast lists and other preset numbers of frequent recipients of FTI.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation:	Email and any attachment that contains sensitive information when transmitted inside and outside of HHS premises shall be encrypted using the user's personal identity verification (PIV) card when possible; if PIV encryption is not feasible, a FIPS 140-2 validated solution must be employed: (i) password protection of files is recommended to add an additional layer of data protection but shall not be used in lieu of encryption solutions, and (ii) password and/or encryption key shall not be included in the same email that contains sensitive information or in separate email, and password/encryption key shall be provided to the recipient separately via text message, verbally, or other out-of-band solution.

Control Reference: 09.w Interconnected Business Information Systems

Control Specification:	Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.
Factor Type:	Organizational
Topics:	Communications and Transmissions; Physical and Facility Security; Policies and Procedures; User Access; Network Security

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation:	Security and business implications are addressed for interconnecting business information assets including: 1. policy and appropriate controls to manage information sharing; 2. excluding categories of sensitive business information and classified documents if the system does not provide an appropriate level of protection; 3. categories of personnel, contractors or business partners allowed to use the system and the locations from which it may be accessed; 4. restricting selected systems and facilities to specific categories of user; and 5. identifying the status of users (e.g., employees of the organization or contractors in directories for the benefit of other users).
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) NIST Cybersecurity Framework v1.1 PR.AC-3 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.DS-5

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians

	Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to FedRAMP Certification Subject to FISMA Compliance Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The organization: 1. Authorizes and approves connections of defined internal information system components or classes of components (defined in the applicable security plan) to the information system; and 2. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated along with their security and business implications. Security and business implications are addressed for interconnecting business information assets including: 1. known vulnerabilities in the administrative and accounting systems where information is shared between different parts of the organization; 2. restricting access to diary information relating to selected individuals (e.g., personnel working on sensitive projects); and 3. vulnerabilities of information in business communication systems (e.g., recording phone calls or conference calls, confidentiality of calls, storage of facsimiles, opening mail, distribution of mail). Interconnected business information systems are linked to other requirements and controls, including: 1. the separation of operational systems from interconnected system; 2. the retention and back-up of information held on the system; and 3. the fallback requirements and arrangements. A baseline is established for basic security hygiene in interconnected systems.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC6.1 CMSRs v3.1 CA-09 (HIGH; MOD) CMSRs v3.1 CM-02 (HIGH; MOD) COBIT 5 DS5.10 COBIT 5 DS5.11 COBIT 5 DSS05.02 COBIT 5 DSS05.03 FedRAMP CA-9 FedRAMP CM-2 IRS Pub 1075 v2016 9.3.5.2 ISO/IEC 27002:2013 13.1.3 ISO/IEC 27799:2016 13.1.3 MARS-E v2 CM-2 NIST Cybersecurity Framework v1.1 DE.AE-1 NIST Cybersecurity Framework v1.1 PR.AC-3 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.AC-5

	NIST Cybersecurity Framework v1.1 PR.IP-1 NIST Cybersecurity Framework v1.1 PR.IP-4 NIST SP 800-53 R4 AC-4[HM]{1} NIST SP 800-53 R4 CA-3(4)[S]{0} NIST SP 800-53 R4 SC-42(2)[S]{0} NIST SP 800-53 R4 SC-42(3)[S]{0} NIST SP 800-53 R4 SC-42[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 CA-9a[M]-0 PCI DSS v3.2.1 1.2

Objective Name: 09.09 Electronic Commerce Services

Control Objective:	Ensure the security of electronic commerce services, and their secure use.

Control Reference: 09.x Electronic Commerce Services

Control Specification:	Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure or modification. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Authorization; Cryptography; Data Loss Prevention; Requirements (Legal and Contractual); Third-parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation:	The confidentiality and integrity for electronic commerce are maintained by ensuring the following: 1. the level of confidence each party requires in each other's claimed identity (e.g., through authentication); 2. authorization processes associated with who may set prices, issue or sign key trading documents; 3. ensuring that trading partners are fully informed of their authorizations; 4. determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key documents, and the non-repudiation of contracts (e.g., associated with tendering and contract processes); 5. the level of trust required in the integrity of advertised price lists; 6. the confidentiality of any covered data or information; 7. the confidentiality and integrity of any order transactions, payment information, delivery address details, and confirmation of receipts; 8. the degree of verification appropriate to check payment information supplied by a customer; 9. selecting the most appropriate settlement form of payment to guard against fraud; 10. the level of protection required to maintain the confidentiality and integrity of order information;

	11. avoidance of loss or duplication of transaction information; 12. liability associated with any fraudulent transactions; and 13. insurance requirements.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) CMSRs v3.1 AU-10 (HIGH) COBIT 5 DS5.11 CSA CCM v3.0.1 DSI-03 MARS-E v2 AU-10 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.DS-2

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: A documented agreement is committed and maintained for electronic commerce arrangements between trading partners on the agreed terms of trading, including details of authorization. Other agreements with information service and value-added network providers are also required. Attacks of the host(s) used for electronic commerce are addressed to provide resilient service(s). The security implications of any network interconnection required for the implementation of electronic commerce services are identified and addressed. Cryptographic controls are used to enhance security, taking into account compliance with legal requirements.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 SC-08 (HIGH; MOD) CMSRs v3.1 SC-08(01) (HIGH; MOD) FedRAMP SC-8 IRS Pub 1075 v2016 9.3.16.6 ISO/IEC 27002:2013 14.1.2 ISO/IEC 27799:2016 14.1.2 MARS-E v2 SC-8 MARS-E v2 SC-8(1) NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 PR.AT-3 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.DS-2 NIST Cybersecurity Framework v1.1 PR.DS-5

Level CMS Implementation Requirements

Level CMS Implementation:	The information system protects against an individual (or process acting on behalf of an individual) from falsely denying having performed a particular action.

Control Reference: 09.y On-line Transactions

Control Specification:	Information involved in online transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Authentication; Communications and Transmissions; Cryptography

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation:	Data involved in electronic commerce and online transactions is checked to determine if it contains covered information. Security is maintained through all aspects of the transaction, ensuring that: 1. user credentials of all parties are valid and verified; 2. the transaction remains confidential; and 3. privacy associated with all parties involved is retained. Protocols used to communicate between all involved parties are secured using cryptographic techniques (e.g., SSL).
Level 1 Control Standard Mapping:	CRR v2016 CM:G2.Q4 CSA CCM v3.0.1 DSI-03 ISO/IEC 27002:2013 14.1.3 ISO/IEC 27799:2016 14.1.3 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.DS-2 NIST Cybersecurity Framework v1.1 PR.DS-5

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records

Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to IRS Pub 1075 Compliance Subject to the EU GDPR
Level 2 Implementation:	Level 1 plus: The use of electronic signatures by each of the parties involved in the transaction is required. The organization ensures the storage of the transaction details are located outside of any publicly accessible environments (e.g., on a storage platform existing on the organization's intranet) and are not retained and exposed on a storage medium directly accessible from the Internet. Where a trusted authority is used (e.g., for the purposes of issuing and maintaining digital signatures and/or digital certificates) security is integrated and embedded throughout the entire end-to-end certificate/signature management process. Communications path between all involved parties is encrypted. The protocols used for communications are enhanced to address any new vulnerability, and the updated versions are adopted as soon as possible.
Level 2 Control Standard Mapping:	CAQH Core Phase 1 153: Eligibility and Benefits Connectivity Rule v1.1.0 Subsection 5.2 CMSRs v3.1 AU-10 (HIGH) CSA CCM v3.0.1 DSI-03 IRS Pub 1075 v2016 Exhibit 10 ISO/IEC 27002:2013 14.1.3 ISO/IEC 27799:2016 14.1.3 MARS-E v2 AU-10 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.DS-2 NIST Cybersecurity Framework v1.1 PR.DS-5

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	All Internet transmissions in a data warehouse are to be encrypted with the use of HTTPS protocol and secure sockets layer encryption based on a certificate that contains a key no less than 128 bits in length, or FIPS 140-2 compliant, whichever is stronger. All sessions are encrypted and provide end-to-end encryption (i.e., from workstation to point of data), as data is at its highest risk during the ETL stages when it enters the warehouse. Web server(s) that receive online transactions in a data warehouse are configured in a demilitarized zone (DMZ) to receive external transmissions but still have some measure of protection against unauthorized intrusion (e.g., by an IDS/IPS). Application server(s) and database server(s) supporting a data warehouse are configured behind the firewalls for optimal security against unauthorized intrusion. Only authenticated applications and users are allowed access to these servers. Transaction data is 'swept' from the web server(s) at frequent intervals, consistent with good system performance, and removed to a secured server behind the firewalls to minimize the risk that these transactions could be destroyed or altered by intrusion.

Control Reference: 09.z Publicly Available Information

Control Specification:	The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.
Factor Type:	Organizational
Topics:	Authorization

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation:	There is a formal approval process before information is made publicly available. In addition, all input provided from the outside to the system is verified and approved. The source (authorship) of publicly available information is stated. The organization ensures that network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications.
Level 1 Control Standard Mapping:	NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.DS-6

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to CMMC Level 1 Subject to CMMC Level 3 Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus:

	The organization: 1. designates individuals authorized to post information onto a publicly accessible information system; 2. trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; 3. reviews the proposed content of information prior to posting onto the publicly accessible information system prior to posting to ensure non-public information is not included; 4. reviews the content on the publicly accessible information systems for nonpublic information bi-weekly; and 5. removes nonpublic information from the publicly accessible information systems, if discovered. The publicly accessible system is tested against weaknesses and failures prior to information being made available. Installation checklist and vulnerability testing are implemented to ensure security baselines and configuration baselines are met or exceeded. Electronic publishing systems, especially those that permit feedback and direct entering of information, are carefully controlled so that: 1. information is obtained in compliance with any data protection legislation; 2. information input to, and processed by, the publishing system will be processed completely and accurately in a timely manner; 3. covered information will be protected during collection, processing, and storage; and 4. access controls to the publishing system do not allow unintended access to networks to which the system is connected. Publicly available health information (as distinct from personal health information) is archived.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC8.1 CMMC v1.0 AC.1.004-1 CMMC v1.0 AC.1.004-2 CMMC v1.0 SC.3.193-1 CMSRs v3.1 AC-22 (HIGH; MOD) CMSRs v3.1 CM-06 (HIGH; MOD) CMSRs v3.1 SC-CMS-2 (HIGH; MOD) COBIT 5 DS7.2 COBIT 5 DSS06.03 FedRAMP AC-22 FedRAMP CM-6 IRS Pub 1075 v2016 9.3.1.17 IRS Pub 1075 v2016 9.3.5.6 ISO/IEC 27001:2013 14.1.2 MARS-E v2 CM-6 NIST 800-171 r2 3.1.22-1 NIST 800-171 r2 3.1.22-2 NIST Cybersecurity Framework v1.1 DE.CM-8 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 ID.RA-1 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.AT-2 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.DS-2 NIST Cybersecurity Framework v1.1 PR.DS-6 NIST Cybersecurity Framework v1.1 PR.IP-1 NIST SP 800-53 R4 AC-22a[HML]{0} NIST SP 800-53 R4 AC-22b[HML]{0} NIST SP 800-53 R4 AC-22c[HML]{0} NIST SP 800-53 R4 AC-22d[HML]{0} NY DOH SSP v3.1 AC-22a[M]-0 NY DOH SSP v3.1 AC-22b[M]-0

	NY DOH SSP v3.1 AC-22c[M]-0 NY DOH SSP v3.1 AC-22d[M]-0

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to FedRAMP Certification Subject to FISMA Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (Supplemental)
Level 3 Implementation:	Level 2 plus: Software, data, and other information requiring a high level of integrity being made available on a publicly available system, are protected by appropriate mechanisms, including digital signatures. The signatures themselves provide a convenient point for either access or denial of service attack and require extra protection. Digital Signatures are protected on a secure, fault-tolerant system (e.g., increased capacity and bandwidth, service redundancy) with protected access and with full auditing.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 SC-05 (HIGH; MOD) CMSRs v3.1 SC-05(02) (HIGH; MOD) FedRAMP SC-5 IRS Pub 1075 v2016 9.3.16.4 ISO/IEC 27002:2013 14.1.2 ISO/IEC 27799:2016 14.1.2 MARS-E v2 SC-5 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.DS-6 NIST Cybersecurity Framework v1.1 PR.DS-8 NIST SP 800-53 R4 SI-7(6)[S]{2}

Level CMS Implementation Requirements

Level CMS Implementation:	Websites are operated within the restrictions addressed in OMB directives M-10-22 "Guidance for Online Use of Web Measurement and Customization Technologies" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications" and applicable CMS and DHHS directives and instruction. The organization monitors the CMS and DHHS security programs to determine if there are any modified directives and instruction.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	The agency must:

	1. Designate individuals authorized to post information onto a publicly accessible information system; 2. Train authorized individuals to ensure that publicly accessible information does not contain FTI; 3. Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that FTI is not included; and 4. Review the content on the publicly accessible information system for FTI, at a minimum, quarterly and remove such information, if discovered.

Objective Name: 09.10 Monitoring

Control Objective:	Ensure information security events are monitored and recorded to detect unauthorized information processing activities in compliance with all relevant legal requirements.

Control Reference: 09.aa Audit Logging

Control Specification:	Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring. *Required for HITRUST Certification CSF v9.6
Factor Type:	System
Topics:	Audit and Accountability; Documentation and Records; Incident Response; User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to HIPAA Security Rule Subject to HITRUST De-ID Framework Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Supplemental Requirements Subject to Texas Health and Safety Code
Level 1 Implementation:	Information systems processing covered and/or confidential information create a secure audit record each time a user accesses, creates, updates, deletes, or archives covered and/or confidential information via the system. Where possible, transaction-level logging/auditing is performed (e.g., on a database system). Where possible, transaction-level logging/auditing is performed (e.g., on a database system). The audit logs include: 1. a unique user identifier; 2. a unique data subject (e.g., client/customer) identifier; 3. the function performed by the user (e.g., log-in, including failed attempts; record creation; access; update; etc.); and 4. the time and date that the function was performed. 5. Logs for operators or administrators also include:

	6. the type of event that occurred (e.g., success or failure); 7. the time at which an event occurred; 8. information about the event (e.g., files handled) or failure (e.g., error occurred, and corrective action taken); 9. the account(s) and administrator(s) or operator(s) involved; and 10. the process(es) involved. Retention for audit logs is specified by the organization and retained accordingly.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(b) 21 CFR Part 11.10(e) 45 CFR Part § 164.312(b) HIPAA.SR-1 45 CFR Part § 164.312(b) HIPAA.SR-2 45 CFR Part § 164.316(b)(1)(ii) HIPAA.SR-1 AICPA 2017 CC2.1 CMSRs v3.1 AR-04 (HIGH; MOD) CMSRs v3.1 AU-03 (HIGH; MOD) CMSRs v3.1 AU-08 (HIGH; MOD) CMSRs v3.1 AU-09 (HIGH; MOD) COBIT 5 DSS05.04 CRR v2016 CM:G2.Q6 CSA CCM v3.0.1 IVS-01 De-ID Framework v1 Audit Logging/Monitoring: General De-ID Framework v1 Retention: Data Retention Policy FedRAMP AU-8(1) FFIEC IS v2016 A.6.20(d) FFIEC IS v2016 A.6.21(b) FFIEC IS v2016 A.6.22(f) FFIEC IS v2016 A.6.27(a) FFIEC IS v2016 A.6.35 HITRUST IRS Pub 1075 v2016 9.3.3.10 IRS Pub 1075 v2016 9.3.3.11 IRS Pub 1075 v2016 9.3.3.4 ISO/IEC 27002:2013 12.4.1 ISO/IEC 27002:2013 12.4.2 ISO/IEC 27002:2013 12.4.3 ISO/IEC 27799:2016 12.4.1 ISO/IEC 27799:2016 12.4.2 ISO/IEC 27799:2016 12.4.3 MARS-E v2 AR-4 MARS-E v2 AU-3 MARS-E v2 AU-8 MARS-E v2 AU-9 NIST Cybersecurity Framework v1.1 DE.CM-1 NIST Cybersecurity Framework v1.1 DE.CM-3 NIST Cybersecurity Framework v1.1 PR.PT-1 NIST SP 800-53 R4 AC-9(3)[S]{0} NIST SP 800-53 R4 AU-14(2)[S]{0} NIST SP 800-53 R4 AU-14[S]{2} NIST SP 800-53 R4 AU-8[HML]{2} NRS 603A.215.1 NY DOH SSP v3.1 AU-11[M]-2 NY DOH SSP v3.1 AU-2.IS.PII1b[M]-0 NY DOH SSP v3.1 AU-2.IS.PII2b[M]-0 NY DOH SSP v3.1 AU-3a[M]-0 NY DOH SSP v3.1 AU-3e[M]-2 NY DOH SSP v3.1 AU-3f[M]-0 OCR Audit Protocol (2016) 164.308(a)(5)(ii)(C) PCI DSS v3.2.1 10.2.1 PCI DSS v3.2.1 10.2.2 PCI DSS v3.2.1 10.3.1 PCI DSS v3.2.1 10.3.2 PCI DSS v3.2.1 10.3.3 PCI DSS v3.2.1 10.3.4 PCI DSS v3.2.1 10.3.5 PCI DSS v3.2.1 10.3.6 PCI DSS v3.2.1 10.3.7 PCI DSS v3.2.1 10.5 PMI DSP Framework DE-1 PMI DSP Framework DE-2

	SR v6.4 28.1-0 SR v6.4 28.2-0 SR v6.4 28a-0 SR v6.4 28b-0 SR v6.4 45b.3-0 SR v6.4 7b.6-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	Subject to 23 NYCRR 500 Subject to CMMC Level 3 Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline
Level 2 Implementation:	Level 1 plus: Messaging systems used to transmit messages containing covered information keep a log of message transmissions, such a log contain the time, date, origin, and destination of the message, but not its content. The organization carefully assesses and determines the retention period for these audit logs, with particular reference to professional standards and legal obligations, in order to enable investigations to be carried out when necessary, and to provide evidence of misuse where necessary. Audit logs include, but are not limited to: 1. dates, times, and details of key events (e.g., log-on and log-off); 2. records of successful and rejected system access attempts; 3. records of successful and rejected data and other resource access attempts; 4. changes to system configuration and procedures for managing configuration changes; 5. use of privileges; 6. use of system utilities and applications; 7. files accessed and the kind of access; 8. network addresses and protocols; 9. alarms raised by the access control system; 10. activation and de-activation of protection systems, including anti-virus systems and intrusion detection systems, and identification and authentication mechanisms; and 11. creation and deletion of system level objects. The organization provides a rationale for why the auditable events are deemed adequate to support after-the-fact investigations of security incidents and which events require auditing on a continuous basis in response to specific situations. The listing of auditable events is reviewed and updated within every 365 days. Information systems' audit logging systems are operational at all times while the information system being audited is available for use. Where necessary for highly sensitive logs, separation of duties and split key access is employed. Audit records are retained for 90 days, and old records archived for 1 year to provide support for after-the-fact investigations of security incidents and to meet regulatory, and the organization's, retention requirements.

Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(b) 21 CFR Part 11.10(e) CIS CSC v7.1 14.9 CMMC v1.0 AU.3.045-0 CMSRs v3.1 AC-06(09) (HIGH; MPD) CMSRs v3.1 AU-02 (HIGH) CMSRs v3.1 AU-02(03) (HIGH) CMSRs v3.1 AU-03 (HIGH; MOD) CMSRs v3.1 AU-05 (HIGH; MOD) CMSRs v3.1 AU-11 (HIGH; MOD) COBIT 5 DSS05.04 CSA CCM v3.0.1 IVS-01 FedRAMP AC-6(9) FedRAMP AU-2 FedRAMP AU-5 FFIEC IS v2016 A.6.21(b) FFIEC IS v2016 A.6.22(f) FFIEC IS v2016 A.6.27(a) FFIEC IS v2016 A.6.35 HITRUST IRS Pub 1075 v2016 9.3.3.11 IRS Pub 1075 v2016 9.3.3.3 IRS Pub 1075 v2016 9.3.3.4 ISO/IEC 27002:2013 12.4.1 ISO/IEC 27002:2013 12.4.2 ISO/IEC 27799:2016 12.4.1 ISO/IEC 27799:2016 12.4.2 MARS-E v2 AC-6(9) MARS-E v2 AU-11 MARS-E v2 AU-2 MARS-E v2 AU-3 MARS-E v2 AU-5 NIST 800-171 r2 3.3.3-0 NIST Cybersecurity Framework v1.1 DE.CM-1 NIST Cybersecurity Framework v1.1 DE.CM-3 NIST Cybersecurity Framework v1.1 ID.SC-4 NIST Cybersecurity Framework v1.1 PR.PT-1 NIST SP 800-53 R4 AU-10(1)b[S]{0} NIST SP 800-53 R4 AU-10[H]{1} NIST SP 800-53 R4 AU-11[HML]{0} NIST SP 800-53 R4 AU-2(3)[HM]{0} NIST SP 800-53 R4 AU-2c[HML]{0} NIST SP 800-53 R4 AU-2d[HML]{0} NIST SP 800-53 R4 AU-6(8)[S]{2} NIST SP 800-53 R4 SA-12(14)[S]{0} NIST SP 800-53 R4 SI-10(1)c[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 AU-11[M]-1 NY DOH SSP v3.1 AU-12a3[M]-2 NY DOH SSP v3.1 AU-12a4[M]-2 NY DOH SSP v3.1 AU-2c[M]-0 NY DOH SSP v3.1 AU-3g[M]-3 NY DOH SSP v3.1 CM-3f[M]-2 PCI DSS v3.2.1 10.2 PCI DSS v3.2.1 10.2.4 PCI DSS v3.2.1 10.2.7 PCI DSS v3.2.1 10.3.1 PCI DSS v3.2.1 10.3.2 PCI DSS v3.2.1 10.3.3 PCI DSS v3.2.1 10.3.5 PCI DSS v3.2.1 10.7 PMI DSP Framework DE-1 PMI DSP Framework PR.DS-5

Level 3 Implementation Requirements

Level 3 Organizational Factors:	
Level 3 System Factors:	Number of interfaces to other systems Greater than 75 Number of transactions per day Greater than 85,000 Number of users of the system(s) Greater than 5,500

Level 3 Regulatory Factors:	Subject to Banking Requirements Subject to CA Civil Code § 1798.81.5 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: 1. Server alerts and error messages; 2. user log-on and log-off (successful or unsuccessful); 3. all system administration activities; 4. modification of privileges and access; 5. start-up and shutdown; 6. application modifications; 7. application alerts and error messages; 8. configuration changes; 9. account creation, modification, or deletion; 10. file creation and deletion; 11. read access to sensitive information; 12. modification to sensitive information; and 13. printing sensitive information. The information system also generates audit records containing the following additional, more detailed, information: 1. Filename accessed; 2. Program or command used to initiate the event; and 3. Source and destination addresses. Disclosures of covered information are recorded. Information type, date, time, receiving party, and releasing party are logged. The organization verifies every 90 days for each extract that the data is erased, or its use is still required. Account creation, modification, disabling, enabling and removal actions are automatically logged and audited providing notification, as required, to appropriate individuals.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(e) AICPA 2017 C1.2 CIS CSC v7.1 4.8 CMSRs v3.1 AC-06(09) (HIGH; MOD) CMSRs v3.1 AR-04 (HIGH; MOD) CMSRs v3.1 AU-02 (HIGH; MOD) CMSRs v3.1 AU-03 (HIGH; MOD) CMSRs v3.1 AU-03(01) (HIGH; MOD) CMSRs v3.1 AU-12 (HIGH; MOD) COBIT 5 DSS05.04 CSA CCM v3.0.1 IVS-01 FedRAMP AC-6(9) FedRAMP AU-3 FedRAMP AU-9 HITRUST IRS Pub 1075 v2016 9.3.3.2 IRS Pub 1075 v2016 9.3.3.4 IRS Pub 1075 v2016 9.4.11 IRS Pub 1075 v2016 9.4.13 IRS Pub 1075 v2016 9.4.18

	IRS Pub 1075 v2016 9.4.3 IRS Pub 1075 v2016 9.4.9 ISO/IEC 27002:2013 12.4.1 ISO/IEC 27799:2016 12.4.1 MARS-E v2 AC-6(9) MARS-E v2 AR-4 MARS-E v2 AU-12 MARS-E v2 AU-3 NIST Cybersecurity Framework v1.1 DE.CM-1 NIST Cybersecurity Framework v1.1 DE.CM-3 NIST Cybersecurity Framework v1.1 PR.PT-1 NIST SP 800-53 R4 AU-14[S]{3} NIST SP 800-53 R4 AU-3(1)[HM]{0} NY DOH SSP v3.1 AU-12a5[M]-1 NY DOH SSP v3.1 AU-2.IS.PII1e[M]-0 NY DOH SSP v3.1 AU-2.IS.PII2e[M]-0 NY DOH SSP v3.1 AU-3(1)a[M]-0 NY DOH SSP v3.1 AU-3(1)b[M]-0 NY DOH SSP v3.1 AU-3(1)c[M]-0 NY DOH SSP v3.1 AU-3.IS.PHI1[M]-1 NY DOH SSP v3.1 AU-3g[M]-2 PMI DSP Framework DE-1 PMI DSP Framework PR.DS-5

Level CIS	Implementation Requirements
Level CIS Implementation:	The organization enables system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. The organization logs all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.

Level CMS	Implementation Requirements
Level CMS Implementation:	The organization audits inspection reports, including a record of corrective actions, and the audit reports are retained by the organization for a minimum of three years from the date the inspection was completed. Audit records are compiled from multiple components throughout the system into a system-wide (logical or physical) audit trail that is time-correlated to within +/- five minutes. The organization centrally manages the content of audit records generated by individual components throughout the information system. A real-time alert is provided when the audit record log is full or there is an authentication or encryption logging failure. The information system provides the capability for defined individuals or roles (defined in the applicable security plan) to change the auditing to be performed on defined information system components (defined in the applicable security plan) based on defined selectable event criteria (defined in the applicable security plan) within minutes.

Level Community Supplemental Reqs 02	Implementation Requirements
Level Community Supplemental Reqs 02 Implementation:	The organization implements a centralized mechanism to log privileged activities, including the use of privileged accounts and grants to privileged groups; and develops alerting rules and investigation procedures to review suspicious activities.

Level FedRAMP	Implementation Requirements

Level FedRAMP Implementation:	The service provider retains audit records on-line for at least 90 days and further preserves audit records off-line for a period that is in accordance with National Archives and Records Administration (NARA) requirements. Audit logging and monitoring is coordinated between the service provider and the organization and is documented and accepted by the Joint Authorization Board (JAB) and Authorizing Official (AO). The listing of auditable events and supporting rational are reviewed and updated periodically within every 365 days or whenever changes in the threat environment are communicated to the service provider by the Joint Authorization Board (JAB). The information system generates audit records containing the following detailed information: (i) session; (ii) connection; or (iii) activity duration. The service provider defines audit record types and are approved and accepted by the Joint Authorization Board (JAB) and Authorizing Official (AO). The information system generates audit records for client-server transactions containing the following detailed information: (i) bytes received and bytes sent; (ii) bytes received and bytes sent; and (iii) bytes received and bytes sent.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	The organization provides an audit record generation capability and audits the following events, at a minimum: 1. Log onto system; 2. Log off of system; 3. Change of password; 4. All system administrator commands, while logged on as system administrator; 5. Switching accounts or running privileged actions from another account; 6. (e.g., Linux/Unix SU or Windows RUNAS); 7. Creation or modification of super-user groups; 8. Subset of security administrator commands, while logged on in the security administrator role; 9. Subset of system administrator commands, while logged on in the user role; 10. Clearing of the audit log file; 11. Startup and shutdown of audit functions; 12. Use of identification and authentication mechanisms (e.g., user ID and password); 13. Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su); 14. Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system; 15. Changes made to an application or database by a batch file; 16. Application-critical record changes; 17. Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility); 18. All system and data interactions concerning FTI; and 19. Additional platform-specific events, as defined in SCSEMs located on the Office of Safeguards website. The organization audits records for the following events in addition to those specified: 1. all successful and unsuccessful authorization attempts; 2. all changes to logical access control authorities (e.g., rights, permissions);

3. all system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services;
4. the audit trail captures the enabling or disabling of audit report generation services; and
5. the audit trail captures command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).

The organization also:

1. allows designated agency officials to select which auditable events are to be audited by specific components of the information system;
2. coordinates the security audit function with other agency entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
3. provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
4. reviews and updates the audited events at a minimum, annually.

Audit logs must enable tracking activities taking place on the system. Pub 1075, Exhibit 9, System Audit Management Guidelines, contains requirements for creating audit-related processes at the operating system, software, and database levels. Auditing must be enabled to the extent necessary to capture access, modification, deletion, and movement of FTI by each unique user. This auditing requirement also applies to data tables or databases, embedded in or residing outside of the application, which contain FTI.

Information systems generate audit records containing details to facilitate the reconstruction of events if unauthorized activity or a malfunction occurs or is suspected in the audit records for audit events identified by type, location, or subject.

Audit logging must be implemented to properly track all email that contains FTI.

Multifunction Devices (MFDs) and its print spoolers have auditing enabled, including the auditing of user access and fax logs (if fax is enabled).

SAN components must maintain an audit trail of access to FTI in the SAN environment.

To use FTI in an 802.11 WLAN environment, the agency must enable security event logging on WLAN components.

Level HIX Implementation Requirements

Level HIX Implementation:

The information system includes the capability to include more detailed information in the audit records for audit events identified by type, location, or subject.

The organization archives old audit records for 10 years to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Audit records are compiled from multiple components throughout the system into a system-wide (logical or physical), time-correlated audit trail.

The organization defines and employs methods for coordinating organization-defined audit information among external organizations when audit information is transmitted across organizational boundaries (typically when using information systems and/or services of external organizations).

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The information system performs an integrity check of software, firmware, and information daily and at system startup.

Level PCI Implementation Requirements	
Level PCI Implementation:	A service provider protects each organization's hosted environment and data by ensuring logging and audit trails are enabled and unique to each organization's (customer's) cardholder data environment and consistent with PCI DSS v3 Requirement 10.

Level SCIDSA Implementation Requirements	
Level SCIDSA Implementation:	All records concerning cybersecurity events are maintained for at least five years from the date of the event and be available for inspection.

Level Title 23 NYCRR Part 500 Implementation Requirements	
Level Title 23 NYCRR Part 500 Implementation:	The covered entity must maintain audit records designed to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operations of the covered entity for three years.

Control Reference: 09.ab Monitoring System Use

Control Specification:	Procedures for monitoring use of information processing systems and facilities shall be established to check for use and effectiveness of implemented controls. The results of the monitoring activities shall be reviewed regularly. *Required for HITRUST Certification CSF v9.6
Factor Type:	System
Topics:	Incident Response; Monitoring; Requirements (Legal and Contractual); User Access

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to CMMC Level 2 Subject to CMMC Level 3 Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Texas Health and Safety Code
Level 1 Implementation:	The organization complies with all relevant legal requirements applicable to its monitoring activities. Items that are monitored include: 1. authorized access; and

	2. unauthorized access attempts. The organization specifies how often audit logs are reviewed, how the reviews are documented, and the specific roles and responsibilities of the personnel conducting the reviews, including the professional certifications or other qualifications required. The organization periodically tests its monitoring and detection processes, remediates deficiencies, and improves its processes. Information collected from multiple sources is aggregated for review.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 201 CMR 17.03(2)(h) CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMMC v1.0 AU.2.044-0 CMMC v1.0 AU.3.048-2 CMSRs v3.1 SI-04 (HIGH; MOD) CRR v2016 VM:G1.Q5 CSA CCM v3.0.1 IVS-01 FedRAMP SI-4 FFIEC IS v2016 A.6.22(f) FFIEC IS v2016 A.6.35 FFIEC IS v2016 A.6.35(c) IRS Pub 1075 v2016 9.3.17.4 MARS-E v2 SI-4 NIST Cybersecurity Framework v1.1 DE.AE-3 NIST Cybersecurity Framework v1.1 DE.DP-2 NIST Cybersecurity Framework v1.1 DE.DP-3 NIST Cybersecurity Framework v1.1 DE.DP-5 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST SP 800-53 R4 SI-4(9)[S]{0} NIST SP 800-53 R4 SI-4f[HML]{0} NY DOH SSP v3.1 SI-4f[M]-0 OCR Audit Protocol (2016) 164.308(a)(1)(ii)(D)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	Subject to 23 NYCRR 500 Subject to CMMC Level 2 Subject to CMMC Level 3 Subject to CMMC Level 4 Subject to CMMC Level 5 Subject to FTC Red Flags Rule Subject to HIPAA Security Rule Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to State of Massachusetts Data Protection Act Subject to Supplemental Requirements
Level 2 Implementation:	Level 1 plus:

Information systems containing covered and/or confidential information are actively provided with automated assets for monitoring events of the system(s), detecting attacks, and analyzing logs and audit trails that:

1. allow the identification of all system users who have accessed, or modified a given record(s) over a given period of time; and
2. allow the identification of all records that have been accessed or modified by a given system user over a given period of time.

The organization monitors (e.g., host-based monitoring) the information system to identify irregularities or anomalies that are indicators of a system malfunction or compromise and help confirm the system is functioning in an optimal, resilient and secure state.

Monitoring devices are strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information. Monitoring devices are also deployed at ad hoc locations within the system to track specific transactions. Additionally, these devices are used to track the impact of security changes to the information system.

The organization deploys NetFlow collection and analysis to DMZ network flows to detect anomalous activity.

The organization:

1. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
2. Reviews physical access logs weekly and upon occurrence of security incidents involving physical security; and
3. Coordinates results of reviews and investigations with the organization's incident response capability.

Monitoring of authorized access includes:

1. the user ID;
2. the date and time of key events;
3. the types of events;
4. the files accessed; and
5. the program/utilities used.

All privileged operations are monitored including:

1. the use of privileged accounts (e.g., supervisor, root, administrator);
2. the system start-up and stop; and
3. I/O device attachment/detachment.

Monitoring of unauthorized access attempts includes:

1. failed or rejected user actions, including attempts to access deactivated accounts;
2. failed or rejected actions involving data and other resources;
3. access policy violations and notifications for network gateways and firewalls; and
4. alerts from proprietary intrusion detection systems.

System alerts or failures are monitored including:

1. console alerts or messages;
2. system log exceptions;
3. network management alarms;
4. alarms raised by the access control system (e.g., intrusion detection, intrusion prevention, or networking monitoring software); and

	5. changes to, or attempts to change, system security settings and controls. The information system provides the capability to automatically process audit records in the information system for events of interest based on selectable event criteria. Systems support audit reduction and report generation that supports expeditious, on-demand review, analysis, reporting and after-the-fact incident investigations of security incidents and do not alter the original content or time marking of audit records.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 16 CFR Part § 681 Appendix A III(b) 45 CFR Part § 164.308(a)(1)(ii)(D) HIPAA.SR-0 45 CFR Part § 164.308(a)(5)(ii)(C) HIPAA.SR-0 45 CFR Part § 164.312(b) HIPAA.SR-3 AICPA 2017 A1.2 AICPA 2017 CC2.1 AICPA 2017 CC7.2 CIS CSC v7.1 12.5 CIS CSC v7.1 12.8 CIS CSC v7.1 13.5 CIS CSC v7.1 15.10 CIS CSC v7.1 16.12 CIS CSC v7.1 16.13 CIS CSC v7.1 6.2 CIS CSC v7.1 8.1 CMMC v1.0 AU.3.052-0 CMMC v1.0 AU.5.055-0 CMMC v1.0 IR.5.102-0 CMMC v1.0 SA.4.171-0 CMMC v1.0 SI.2.217-1 CMMC v1.0 SI.5.222-0 CMMC v1.0 SI.5.223-0 CMSRs v3.1 AR-04 (HIGH) CMSRs v3.1 AR-04 (HIGH; MOD) CMSRs v3.1 AU-02 (HIGH; MOD) CMSRs v3.1 AU-03 (HIGH; MOD) CMSRs v3.1 AU-07 (HIGH; MOD) CMSRs v3.1 AU-07(01) (HIGH) CMSRs v3.1 PE-06 (HIGH) CMSRs v3.1 PE-06 (HIGH; MOD) CMSRs v3.1 SI-04 (HIGH; MOD) CMSRs v3.1 SI-04(02) (HIGH; MOD) COBIT 5 DS5.7 COBIT 5 DSS05.05 De-ID Framework v1 Audit Logging/Monitoring: General FedRAMP AU-2 FedRAMP AU-7 FedRAMP PE-6 FedRAMP SI-4 FedRAMP SI-4(2) FFIEC IS v2016 A.6.20(d) FFIEC IS v2016 A.6.21(f) FFIEC IS v2016 A.6.21(g) FFIEC IS v2016 A.6.22(f) FFIEC IS v2016 A.6.35 FFIEC IS v2016 A.6.35(c) FFIEC IS v2016 A.8.1(h) FFIEC IS v2016 A.8.5(a) IRS Pub 1075 v2016 4.3.2 IRS Pub 1075 v2016 9.3.11.6 IRS Pub 1075 v2016 9.3.17.4 IRS Pub 1075 v2016 9.3.3.3 IRS Pub 1075 v2016 9.3.3.4 IRS Pub 1075 v2016 9.3.3.8 ISO/IEC 27002:2013 12.4.1 ISO/IEC 27799:2016 12.4.1 MARS-E v2 AR-4 MARS-E v2 AU-2 MARS-E v2 AU-3 MARS-E v2 AU-7 MARS-E v2 AU-7(1) MARS-E v2 PE-6

	MARS-E v2 SI-4 MARS-E v2 SI-4(2) NIST 800-171 r2 3.14.7-1 NIST 800-171 r2 3.3.6-0 NIST Cybersecurity Framework v1.1 DE.AE-2 NIST Cybersecurity Framework v1.1 DE.CM-1 NIST Cybersecurity Framework v1.1 DE.CM-7 NIST Cybersecurity Framework v1.1 DE.DP-2 NIST Cybersecurity Framework v1.1 PR.PT-1 NIST Cybersecurity Framework v1.1 RS.CO-3 NIST SP 800-53 R4 AC-4(9)[S]{0} NIST SP 800-53 R4 AU-6(1)[HM]{0} NIST SP 800-53 R4 AU-6(6)[H]{1} NIST SP 800-53 R4 AU-6a[HML]{0} NIST SP 800-53 R4 AU-7[HM]{0} NIST SP 800-53 R4 PE-6c[HML]{0} NIST SP 800-53 R4 SI-4(20)[S]{0} NIST SP 800-53 R4 SI-4c[HML]{0} NY DOH SSP v3.1 AU-12a[M]-0 NY DOH SSP v3.1 AU-12a1[M]-0 NY DOH SSP v3.1 AU-2.IS.PII1a[M]-0 NY DOH SSP v3.1 AU-2.IS.PII2a[M]-0 NY DOH SSP v3.1 AU-7[M]-0 NY DOH SSP v3.1 AU-7a[M]-3 NY DOH SSP v3.1 PE-6c[M]-0 NY DOH SSP v3.1 SI-4a[M]-0 NY DOH SSP v3.1 SI-4a2[M]-1 NY DOH SSP v3.1 SI-4b[M]-1 NY DOH SSP v3.1 SI-4c1[M]-0 PMI DSP Framework DE-2 PMI DSP Framework PR.DS-5 SR v6.4 17.2-1 SR v6.4 17.8-0 SR v6.4 43-0

Level 3 Implementation Requirements

Level 3 Organizational Factors:	
Level 3 System Factors:	Number of interfaces to other systems Greater than 75 Number of transactions per day Greater than 85,000 Number of users of the system(s) Greater than 5,500
Level 3 Regulatory Factors:	Subject to Banking Requirements Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 2 Subject to CMMC Level 3 Subject to CMMC Level 4 Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to HITRUST De-ID Framework Requirements Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to Supplemental Requirements Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus:

Unauthorized remote connections to the information systems are monitored and reviewed at least quarterly, and appropriate action is taken if an unauthorized connection is discovered.

The results of monitoring activities are reviewed daily, through the use of automated tools, for:

1. all security events;
2. logs of all critical system components; and
3. logs of all servers that perform security functions like intrusion detection system (IDS), intrusion prevention system (IPS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).

The automated tools generate alert notification for technical staff review and assessment.

The organization reviews logs of all other system components periodically based on its policies and risk management strategy, as determined by the organization's annual risk assessment.

System records are reviewed for:

1. initialization sequences;
2. log-ons and errors;
3. system processes and performance; and
4. system resources utilization.

The reviews are conducted daily, and the results used to determine anomalies on demand. An alert notification is generated for technical personnel to review and analyze.

Suspicious activity or suspected violations on the information system identified during the review process are investigated, with findings reported to appropriate officials and appropriate actions taken in accordance with the incident response or organizational policies.

Manual reviews of system audit records are performed randomly on demand, but at least once every 30 days.

The organization employs automated mechanisms to integrate the audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

The organization employs automated tools to support near real-time analysis of events and maintain an audit log to track prohibited sources and services. Inbound and outbound communications are monitored at an organization-defined frequency for unusual or unauthorized activities or conditions.

The organization specifies the permitted actions for information system processes, roles, and/or users associated with review, analysis, and reporting of audit records (e.g., read, write, execute, append, and delete).

The organization deploys a change-detection mechanism (e.g., file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; configures the software to perform critical file comparisons at least weekly and responds to any alerts generated.

The information system provides near-real-time alerts when the following indications of compromise or potential compromise occur:

1. presence of malicious code;
2. unauthorized export of information;
3. signaling to an external information system; or

	4. potential intrusions. The organization analyzes and correlates audit records across different repositories using a security information and event management (SIEM) tool or log analytics tools for log aggregation and consolidation from multiple systems/machines/devices and correlates this information with input from non-technical sources to gain and enhance organization-wide situational awareness. Using the SIEM tool, the organization (system administrators and security personnel) devises profiles of common events from given systems/machines/devices so that it can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC2.1 AICPA 2017 CC7.2 CIS CSC v7.1 6.6 CIS CSC v7.1 6.7 CMMC v1.0 AU.3.051-0 CMMC v1.0 AU.4.053-0 CMMC v1.0 AU.4.054-0 CMMC v1.0 SI.2.217-2 CMSRs v3.1 AU-06 (HIGH; MOD) CMSRs v3.1 AU-06(01) (HIGH; MOD) CMSRs v3.1 AU-06(03) (HIGH; MOD) CMSRs v3.1 AU-06(05) (HIGH) CMSRs v3.1 AU-06(06) (HIGH) CMSRs v3.1 AU-07(01) (HIGH; MOD) CMSRs v3.1 SI-03 (HIGH) CMSRs v3.1 SI-04 (HIGH; MOD) CMSRs v3.1 SI-04(02) (HIGH; MOD) CMSRs v3.1 SI-04(03) (HIGH; MOD) CMSRs v3.1 SI-04(04) (HIGH; MOD) CMSRs v3.1 SI-04(05) (HIGH; MOD) CMSRs v3.1 SI-07(02) (HIGH) COBIT 5 DS5.9 COBIT 5 DSS05.01 COBIT 5 DSS05.07 CRR v2016 IM:G2.Q2 CSA CCM v3.0.1 IVS-01 De-ID Framework v1 Audit Logging/Monitoring: Aberrant and Inappropriate Use FedRAMP AC-17 FedRAMP AU-6 FedRAMP AU-6(1) FedRAMP AU-6(3) FedRAMP AU-7(1) FedRAMP SI-3 FedRAMP SI-4 FedRAMP SI-4(16) FedRAMP SI-4(2) FedRAMP SI-4(4) FedRAMP SI-4(5) FFIEC IS v2016 A.6.35(d) FFIEC IS v2016 A.8.1(h) IRS Pub 1075 v2016 6.4.1 IRS Pub 1075 v2016 9.3.16.6 IRS Pub 1075 v2016 9.3.17.3 IRS Pub 1075 v2016 9.3.17.4 IRS Pub 1075 v2016 9.3.3.7 IRS Pub 1075 v2016 9.3.3.8 IRS Pub 1075 v2016 9.4.14 IRS Pub 1075 v2016 9.4.15 IRS Pub 1075 v2016 9.4.18 IRS Pub 1075 v2016 Exhibit 10 MARS-E v2 AC-17 MARS-E v2 AU-6 MARS-E v2 AU-6(1) MARS-E v2 AU-6(3) MARS-E v2 AU-7(1) MARS-E v2 SI-3 MARS-E v2 SI-4 MARS-E v2 SI-4(1) MARS-E v2 SI-4(2)

	MARS-E v2 SI-4(4) MARS-E v2 SI-4(5) NIST 800-171 r2 3.14.7-2 NIST 800-171 r2 3.3.5-0 NIST Cybersecurity Framework v1.1 DE.AE-2 NIST Cybersecurity Framework v1.1 DE.AE-3 NIST Cybersecurity Framework v1.1 DE.CM-1 NIST Cybersecurity Framework v1.1 DE.CM-4 NIST Cybersecurity Framework v1.1 DE.CM-7 NIST Cybersecurity Framework v1.1 DE.DP-2 NIST Cybersecurity Framework v1.1 DE.DP-4 NIST Cybersecurity Framework v1.1 ID.RA-1 NIST Cybersecurity Framework v1.1 PR.PT-1 NIST Cybersecurity Framework v1.1 RS.AN-1 NIST Cybersecurity Framework v1.1 RS.CO-2 NIST SP 800-53 R4 AC-20(4)[S]{1} NIST SP 800-53 R4 AU-12(2)[S]{0} NIST SP 800-53 R4 AU-12a[HML]{0} NIST SP 800-53 R4 AU-12b[HML]{0} NIST SP 800-53 R4 AU-2a[HML]{0} NIST SP 800-53 R4 AU-2b[HML]{0} NIST SP 800-53 R4 AU-3(2)[H]{0} NIST SP 800-53 R4 AU-5(2)[H]{0} NIST SP 800-53 R4 AU-6(3)[HM]{0} NIST SP 800-53 R4 AU-6(4)[S]{0} NIST SP 800-53 R4 AU-6(7)[S]{0} NIST SP 800-53 R4 AU-6(9)[S]{0} NIST SP 800-53 R4 AU-7(2)[S]{0} NIST SP 800-53 R4 SA-18(2)[S]{2} NIST SP 800-53 R4 SI-3(8)[S]{2} NIST SP 800-53 R4 SI-4(13)[S]{0} NIST SP 800-53 R4 SI-4(16)[S]{0} NIST SP 800-53 R4 SI-4(17)[S]{1} NIST SP 800-53 R4 SI-4(2)[HM]{0} NIST SP 800-53 R4 SI-4(3)[S]{0} NIST SP 800-53 R4 SI-4(4)[HM]{0} NIST SP 800-53 R4 SI-4b[HML]{0} NIST SP 800-53 R4 SI-7(8)[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 AC-17[M]-1 NY DOH SSP v3.1 AU-12c[M]-0 NY DOH SSP v3.1 AU-6(3)[M]-0 NY DOH SSP v3.1 AU-6(6)[HN]-1 NY DOH SSP v3.1 AU-7(1)[M]-0 NY DOH SSP v3.1 CA-7b[M]-1 NY DOH SSP v3.1 SC-7.IS4d[M]-2 NY DOH SSP v3.1 SI-4(2)[M]-0 NY DOH SSP v3.1 SI-4(4)[M]-1 NY DOH SSP v3.1 SI-4.IS3[HML]-1 NY DOH SSP v3.1 SI-4.IS3[HML]-2 NY DOH SSP v3.1 SI-4a2[M]-2 NY DOH SSP v3.1 SI-4b[M]-2 PCI DSS v3.2.1 10.6 PCI DSS v3.2.1 10.6.1 PCI DSS v3.2.1 10.6.3 PCI DSS v3.2.1 11.5 PMI DSP Framework DE-3 PMI DSP Framework PR.DS-5 SR v6.4 32a-1 SR v6.4 32a-2

Level CIS Implementation Requirements

Level CIS Implementation:	The organization configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected. The organization monitors all traffic leaving the organization (e.g., through the use of a proxy server as required in 01.o) to detect any unauthorized use of encryption, terminate the connection and take corrective action, (e.g., discipline the responsible party IAW 02.f, remediate the infected system).

	The organization treats enterprise access from VLANs with BYOD systems or other untrusted devices (e.g., legacy medical devices) as untrusted, and filters and audits this access accordingly. The organization profiles each user's typical account usage by determining normal time-of-day access and access duration and generates reports that indicate users who have logged in during unusual hours or have exceeded their normal login duration, which includes flagging the use of the user's credentials from a computer other than computers on which the user generally works. Network boundary devices, including firewalls, network-based IPS, and inbound and outbound proxies, are configured to verbosely log all traffic (both allowed and blocked) arriving at the device, which at a minimum include the full packet header information and payload of the traffic destined for or passing through the network perimeter. The organization employs automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events are sent to enterprise anti-malware administration tools and event log servers. The organization uses network-based DLP solutions to monitor and control the flow of data within the network. Any anomalies that exceed the normal traffic patterns are noted and appropriate action is taken to address them. The network-based DLP solutions are also used to monitor for sensitive information (e.g., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel. The organization uses host-based data loss prevention (DLP) to enforce ACLs even when data is copied off a server. The organization controls and monitors any user or system accounts used to perform penetration testing to make sure they are only being used for legitimate purposes and are removed or restored to normal function after testing is over.

Level CMMC Implementation Requirements	
Level CMMC Implementation:	The organization establishes and maintains a security operations center capability that facilitates 24/7 incident detection and response.

Level CMS Implementation Requirements	
Level CMS Implementation:	The organization: 1. monitors events on the information system in accordance with the current Risk Management Handbook (RMH), Volume II, Procedure 7.2, Incident Handling, and detect information system attacks; 2. heightens the level of information system monitoring activity whenever there is an indication of increased risk to CMS operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information. The organization monitors physical access to the information system, in addition to the physical access monitoring of the facility, at defined physical spaces (defined in the applicable security plan) containing a concentration of information system components (e.g., server rooms, media storage areas, data and communications centers, etc.).

	The organization: 1. Monitors information system accounts for atypical use; and 2. Reports atypical usage of information system accounts to defined personnel or roles (defined in the applicable security plan), and if necessary, incident response team. The organization integrates analysis of audit records with analysis of (one-or-more, defined in the applicable security plan): vulnerability scanning information; performance data; information system monitoring information; and/or other defined data/information (defined in the applicable security plan) collected from other sources, to further enhance the ability to identify inappropriate or unusual activity. The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation:	The organization monitors information system accounts, including privileged accounts for atypical use and reports atypical usage to defined personnel or roles. The organization reviews audit records at least once every seven days for unusual, unexpected, or suspicious behavior. The information system notifies designated organization officials of detected suspicious events and take necessary actions to address suspicious events. Coordination between service provider and consumer is documented and accepted by the Joint Authorization Board (JAB) and Authorizing Official (AO). In multi-tenant environments, capability and means for providing review, analysis, and reporting to consumer for data pertaining to consumer is documented. The organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system (IDS).

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation:	All requests for return information, including receipt and/or disposal of returns or return information, are maintained in a log. Report findings from the review and analysis of information system audit records according to the agency incident response policy. If the finding involves a potential unauthorized disclosure of FTI, the appropriate special agent-in-charge, Treasury Inspector General for Tax Administration (TIGTA), and the IRS Office of Safeguards must be contacted, as described in Section 10.0, Reporting Improper Inspections or Disclosures. Intrusion-detection software is installed and maintained to monitor networks for any unauthorized attempt to access tax data in a data warehouse. The organization must employ automated mechanisms to alert security personnel of inappropriate or unusual activities with security implications, and implement host-based monitoring mechanisms (e.g., Host intrusion prevention system (HIPS)) on information systems that receive, process, store, or transmit FTI. The information system must notify designated agency officials of detected suspicious events and take necessary actions to address suspicious events.

	The agency ensures that audit reports are created and reviewed for data warehousing-related access attempts. If a query is submitted, the audit log must identify the actual query made, the originator of the query, and relevant time and stamp information. A security administrator periodically collects and reviews audit logs from Multifunction Devices (MFDs) and print spoolers. The organization reviews the audit logs (trails) of SAN components on a regular basis to track access to FTI in the SAN environment. To use a virtual environment that receives, processes, stores, or transmits FTI, the agency must ensure virtualization providers must be able to monitor for threats and other activity that is occurring within the virtual environment - this includes being able to monitor the movement of FTI into and out of the virtual environment. To use a VoIP network that provides FTI to a customer, the agency must be able to track and audit all FTI-applicable conversations and access. To use FTI in an 802.11 WLAN, the agency must deploy wireless intrusion detection to monitor for unauthorized access.

Level HIX Implementation Requirements

Level HIX Implementation:	Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than once within a 24-hour period. Generate alerts for technical personnel review and assessment. Use automated utilities to review audit records at least once every seven days for unusual, unexpected, or suspicious behavior. Inspect administrator groups on demand but at least once every 14 days to ensure unauthorized administrator accounts have not been created. The organization complies with HHS privacy oversight monitoring and auditing policies and procedures. For service providers, the organization reviews and analyzes information system audit records at least weekly for indications of inappropriate or unusual activity, and reports findings to designated organizational officials. The organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system (IDS).

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The information system alerts pre-defined personnel or roles (defined in the applicable security plan) when the following indications of compromise or potential compromise occur: (i) presence of malicious code; (ii) unauthorized export of information; (iii) signaling to an external information system; or (iv) potential intrusions. The organization implements CMS-required host-based monitoring mechanisms on all systems, appliances, devices, services, and applications. The organization monitors systems, appliances, devices, and applications (including databases).

	When supported by the underlying operating system, the information system notifies the user, upon successful logon (access) to the system, of the date and time of the last logon (access). When supported by the underlying operating system, the information system notifies the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.

Level PCI	Implementation Requirements
Level PCI Implementation:	The organization reviews, at least daily, the logs of all system components that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD), or that could impact the security of CHD and/or SAD. When being assessed as a service provider, the organization implements a process for the timely detection and reporting of failures of critical security control systems including, but not limited to, failure of: (i) firewalls; (ii) IDS/IPS; (iii) file integrity monitoring; (iv) anti-virus; (v) physical access controls; (vi) logical access controls; (vii) audit logging mechanisms; and (viii) segmentation controls (if used). When being assessed as a service provider, the organization responds to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: (i) restoring security functions; (ii) identifying and documenting the duration (date and time, start to end) of the security failure; (iii) identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause (iv) identifying and addressing any security issues that arose during the failure (v) performing a risk assessment to determine whether further actions are required as a result of the security failure; (vi) implementing controls to prevent cause of failure from reoccurring; and (vii) resuming monitoring of security controls.

Level Supplemental Requirements	Implementation Requirements
Level Supplemental Requirements Implementation:	The organization reviews audit records at least once every seven days for unusual, unexpected, or suspicious behavior.

Control Reference: 09.ac Protection of Log Information

Control Specification:	Logging systems and log information shall be protected against tampering and unauthorized access.
Factor Type:	System
Topics:	Audit and Accountability; Documentation and Records; User Access

Level 1	Implementation Requirements
Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to CMMC Level 3 Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High)

	Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline
Level 1 Implementation:	Access to system audit tools and audit trails is safeguarded from unauthorized access and use to prevent misuse or compromise of logs.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMMC v1.0 AU.3.049-1 CMSRs v3.1 AU-09 (HIGH; MOD) FedRAMP AU-9 FFIEC IS v2016 A.6.21(b) FFIEC IS v2016 A.6.35(b) IRS Pub 1075 v2016 9.3.3.10 ISO/IEC 27002:2013 12.4.2 ISO/IEC 27002:2013 12.4.3 ISO/IEC 27799:2016 12.4.2 ISO/IEC 27799:2016 12.4.3 MARS-E v2 AU-9 NIST 800-171 r2 3.3.8-1 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST SP 800-53 R4 AU-9(5)[S]{1} NIST SP 800-53 R4 AU-9(6)[S]{0} NIST SP 800-53 R4 AU-9[HML]{0} NY DOH SSP v3.1 AU-9[M]-1 PMI DSP Framework DE-2

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CMMC Level 3 Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline
Level 2 Implementation:	Level 1 plus: Access to audit tools and audit trails is limited to those with a job-related need. Authorized and unauthorized access attempts to the audit system and audit trails are logged and protected from modification. Controls protect against unauthorized changes and operational problems with the logging system(s) including: 1. promptly back up audit trail files to a centralized log server or media that is difficult to alter; 2. alterations to the message types that are recorded (e.g., write-once media); and 3. log files being edited or deleted. The organization authorizes access to management of audit functionality to a specific subset of privileged users defined by the organization.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMMC v1.0 AU.3.049-2 CMSRs v3.1 AU-09 (HIGH; MOD) COBIT 5 DSS05.07 FedRAMP AU-9 FFIEC IS v2016 A.6.21(b)

	IRS Pub 1075 v2016 9.3.3.10 MARS-E v2 AU-9 NIST 800-171 r2 3.3.8-2 NIST Cybersecurity Framework v1.1 PR.DS-6 NIST Cybersecurity Framework v1.1 PR.PT-1 NIST SP 800-53 R4 AU-9(1)[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 AU-12(3).NYS[HN]-0 NY DOH SSP v3.1 AU-12a3[M]-1 NY DOH SSP v3.1 AU-12a4[M]-1 NY DOH SSP v3.1 AU-9[M]-2 PCI DSS v3.2.1 10.2.3 PCI DSS v3.2.1 10.5

Level 3 Implementation Requirements

Level 3 Organizational Factors:	
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 3 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: The organization implements file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert) and responds to any alerts generated. The information system: 1. Alerts defined personnel or roles (defined in the applicable security plan) in the event of an audit processing failure; and 2. Takes the following additional actions in response to an audit failure: 3. Shutdown the information system, 4. Stop generating audit records, or 5. Overwrite the oldest records, in the case that storage media is unavailable. Write logs for external-facing technologies (wireless, firewalls, DNS, mail) onto a secure, centralized log server or media device on the internal LAN.
Level 3 Control Standard Mapping:	CMMC v1.0 AU.3.046-0 NIST 800-171 r2 3.3.4-0 NIST Cybersecurity Framework v1.1 DE.CM-1 NIST Cybersecurity Framework v1.1 PR.DS-6 NIST Cybersecurity Framework v1.1 PR.PT-1 NRS 603A.215.1 NY DOH SSP v3.1 AU-5a[M]-3 NY DOH SSP v3.1 AU-7b[M]-0 PCI DSS v3.2.1 10.5.4 PCI DSS v3.2.1 10.5.5 PCI DSS v3.2.1 11.5

Level CIS Implementation Requirements

Level CIS Implementation:	The organization ensures that all systems that store logs have adequate storage space for the logs generated.

Level CMS Implementation Requirements

Level CMS Implementation:	The information system provides a warning to defined personnel, roles, and/or locations (defined in the applicable security plan), within a defined time period (defined in the applicable security plan), when allocated audit record storage volume reaches 80% of repository maximum audit record storage capacity. The information system provides an alert in real time to defined personnel, roles, and/or locations (defined in the applicable security plan) when the following audit failure events occur: 1. Record log is full; 2. Authentication logging failure; and 3. Encryption logging failure. The information system backs up audit records at least weekly onto a physically different system or system component than the system or component being audited. The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The information system backs up audit records at least weekly onto a physically different system or system component than the system or component being audited.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	The information system must monitor system operational status using operating system or system audit logs and verify functions and performance of the system. Logs are able to identify where system process failures have taken place and provide information relative to corrective actions to be taken by the system administrator. The information system does not shut down the system, stop the generation of audit reports or overwrite the oldest records in the event of an audit failure or audit storage capacity issue. The agency must employ mechanisms for coordinating the access and protection of audit information among external organizations when audit information is transmitted across agency boundaries. For additional requirements, see IRS Pub 1075 v2014 9.4.1 for cloud computing environments and 5.4 for consolidated data centers.

Level HIX Implementation Requirements

Level HIX Implementation:	The information system provides a warning to defined personnel, roles, and/or locations (defined in the applicable security plan), within a defined time period (defined in the applicable security plan), when allocated audit record storage volume reaches 80% of repository maximum audit record storage capacity.

Control Reference: 09.ad Administrator and Operator Logs

Control Specification:	System administrator and system operator activities shall be logged and regularly reviewed. *Required for HITRUST Certification CSF v9.6
Factor Type:	System
Topics:	Audit and Accountability; Documentation and Records; Monitoring

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to Supplemental Requirements Subject to Texas Health and Safety Code Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	Organizations ensure that proper logging is enabled in order to audit administrator activities. System administrator and operator logs are reviewed on a regular basis.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CIS CSC v7.1 6.2 CMSRs v3.1 AR-04 (HIGH; MOD) CMSRs v3.1 AU-02 (HIGH; MOD) CMSRs v3.1 AU-06 (HIGH; MOD) FedRAMP AU-12 FedRAMP AU-2 FedRAMP AU-6 FFIEC IS v2016 A.6.35 FFIEC IS v2016 A.6.35(c) IRS Pub 1075 v2016 9.3.3.3 IRS Pub 1075 v2016 9.3.3.7 ISO/IEC 27002:2013 12.4.1 ISO/IEC 27002:2013 12.4.3 ISO/IEC 27799:2016 12.4.1 ISO/IEC 27799:2016 12.4.3 MARS-E v2 AU-2 MARS-E v2 AU-6 NIST Cybersecurity Framework v1.1 ID.SC-4 NIST Cybersecurity Framework v1.1 PR.PT-1 NRS 603A.215.1 NY DOH SSP v3.1 AU-2.IS3[M]-0 PCI DSS v3.2.1 10.2.2 SR v6.4 7b.5-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	

Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day Greater than 85,000 Number of users of the system(s) Greater than 5,500
Level 2 Regulatory Factors:	Subject to Banking Requirements
Level 2 Implementation:	Level 1 plus: An intrusion detection system managed outside of the control of system and network administrators is used to monitor system and network administration activities for compliance.
Level 2 Control Standard Mapping:	CSA CCM v3.0.1 IVS-01 FFIEC IS v2016 A.6.35(c) ISO/IEC 27002:2013 12.4.3 ISO/IEC 27799:2016 12.4.3 NIST Cybersecurity Framework v1.1 PR.PT-1

Control Reference: 09.ae Fault Logging

Control Specification:	Faults shall be logged, analyzed, and appropriate remediation action taken.
Factor Type:	System
Topics:	Audit and Accountability; Documentation and Records; Incident Response

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to Texas Health and Safety Code
Level 1 Implementation:	Faults reported by users or by system programs related to problems with information processing or communications systems are logged. There are clear rules for handling reported faults including: 1. review of fault logs by authorized personnel in an expeditious manner to ensure that faults have been satisfactorily resolved; and 2. review of corrective measures to ensure that controls have not been compromised, and that the action taken is fully authorized. Error logging is enabled if this system function is available.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 AU-02 (HIGH; MOD) COBIT 5 DSS05.07 CSA CCM v3.0.1 IVS-01 FedRAMP AU-2 IRS Pub 1075 v2016 9.3.3.3 ISO/IEC 27002:2013 12.4.1 ISO/IEC 27799:2016 12.4.1 MARS-E v2 AU-2 NIST Cybersecurity Framework v1.1 PR.PT-1

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	
Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The information system: 1. identifies potentially security-relevant error conditions; 2. generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries in error logs and administrative messages that could be exploited by adversaries; and 3. reveals error messages only to authorized personnel. The information system provides automated real-time alerts when faults or errors occur. Covered information is not listed in the logs or associated administrative messages.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 A1.2 CIS CSC v7.1 18.5 CMSRs v3.1 AU-05(02) (HIGH) CMSRs v3.1 SI-11 (HIGH; MOD) COBIT 5 DSS05.07 FedRAMP AU-12 FedRAMP SI-11 IRS Pub 1075 v2016 9.3.17.8 IRS Pub 1075 v2016 9.3.3.6 MARS-E v2 SI-11 NIST Cybersecurity Framework v1.1 DE.DP-4 NIST Cybersecurity Framework v1.1 PR.PT-1 NIST SP 800-53 R4 SC-36(1)[S]{0} NIST SP 800-53 R4 SC-7(23)[S]{0} NIST SP 800-53 R4 SI-11[HM]{0} NY DOH SSP v3.1 AU-5(1).NYSa[HN]-3 NY DOH SSP v3.1 AU-5(2).NYSa[HN]-2 NY DOH SSP v3.1 AU-5(2)b[HN]-0 NY DOH SSP v3.1 AU-5a[M]-1 NY DOH SSP v3.1 SI-11.PII[M]-0 NY DOH SSP v3.1 SI-11a[M]-0 NY DOH SSP v3.1 SI-11b[M]-0

Control Reference:09.af Clock Synchronization

Control Specification:	The clocks of all relevant information processing systems within the organization or security domain shall be synchronized with an agreed accurate time source to support tracing and reconstitution of activity timelines.

Factor Type:	System
Topics:	Audit and Accountability; Requirements (Legal and Contractual)

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to CMMC Level 2 Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	The organization synchronizes all system clocks and times where a computer or communications device has the capability to operate a real-time clock, which is set to an agreed standard received from industry-accepted time sources, either Coordinated Universal Time (UTC) or International Atomic Time and is accurate to within 30 seconds. The correct interpretation of the date/time format is used to ensure that the timestamp reflects the real date/time (e.g., daylight savings). The information system's internal information system clocks synchronize daily and at system boot to one or more authoritative sources (e.g., NIST Internet Time Servers or the U.S. Naval Observatory Stratum-1 NTP servers) when the time difference is greater than 30 seconds.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMMC v1.0 AU.2.043-0 CMSRs v3.1 AU-08 (HIGH; MOD) CMSRs v3.1 AU-08(01) (HIGH; MOD) CSA CCM v3.0.1 IVS-03 FedRAMP AU-8 FedRAMP AU-8(1) IRS Pub 1075 v2016 9.3.3.9 ISO/IEC 27002:2013 12.4.4 ISO/IEC 27799:2016 12.4.4 MARS-E v2 AU-8 MARS-E v2 AU-8(1) NIST 800-171 r2 3.3.7-0 NIST Cybersecurity Framework v1.1 PR.PT-1 NIST SP 800-53 R4 AU-8(1)[HM]{0} NIST SP 800-53 R4 AU-8(2)[S]{0} NIST SP 800-53 R4 AU-8[HML]{1} NRS 603A.215.1 NY DOH SSP v3.1 AU-8(1)b[M]-0 NY DOH SSP v3.1 AU-8b[M]-1 NY DOH SSP v3.1 AU-8b[M]-2 PCI DSS v3.2.1 10.4 PCI DSS v3.2.1 10.4.1 PCI DSS v3.2.1 10.4.3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	

Level 2 System Factors:	Number of interfaces to other systems 25 to 75 Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to PCI Compliance
Level 2 Implementation:	Level 1 plus: Time data is protected according to the organization's access controls (see 01.c) and logging controls (see 09.ad).
Level 2 Control Standard Mapping:	NIST Cybersecurity Framework v1.1 PR.PT-1 NRS 603A.215.1 PCI DSS v3.2.1 10.4.2

Level CIS Implementation Requirements

Level CIS Implementation:	The organization uses at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The information system compares internal clocks at least hourly with the NIST Internet Time Service (see https://www.nist.gov/pml/time-and-frequency-division/services/internet-time-service-its for more information). The service provider selects primary and secondary time servers used by the NIST Internet Time Service. The secondary server is selected from a different geographic region than the primary server. Further, the service provider synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The information system compares the internal information system clocks no less often than daily and at system boot with one or more of the following federally maintained NTP stratum-1 servers: (i) NIST Internet Time Servers (http://tf.nist.gov/tf-cgi/servers.cgi); (ii) U.S. Naval Observatory Stratum-1 NTP Servers (http://tycho.usno.navy.mil/ntp.html); and (iii) CMS designated internal NTP time servers providing an NTP Stratum-2 service to the above servers.

Control Category: 10.0 - Information Systems Acquisition, Development, and Maintenance

Objective Name: 10.01 Security Requirements of Information Systems

Control Objective:	To ensure that security is an integral part of information systems.

Control Reference: 10.a Security Requirements Analysis and Specification

Control Specification:	Statements of business requirements for new information systems (developed or purchased), or enhancements to existing information systems shall specify the requirements for security controls. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Documentation and Records; Requirements (Legal and Contractual); Risk Management and Assessments; Services and Acquisitions

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline
Level 1 Implementation:	The organization develops, disseminates, and reviews/updates annually: 1. a formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls. Specifications for the security control requirements include that security controls be incorporated in the information system, supplemented by manual controls as needed. These considerations are applied when evaluating software packages, developed or purchased. Security requirements and controls reflect the business value of the information assets involved (see 7.d), and the potential business damage that might result from a failure or absence of security. For purchased commercial product, a formal acquisition process is followed. Contracts with the supplier include the identified security requirements. Where the security functionality in a proposed product does not satisfy the specified requirement, then the risk introduced, and associated controls are reconsidered prior to purchasing the

	product. Where additional functionality is supplied, and causes a security risk, this is disabled or mitigated through application of additional controls. The organization requires developers of information systems, components, and services to identify (document) early in the system development life cycle, the functions ports, protocols, and services intended for organizational use.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) AICPA 2017 CC3.1 CMSRs v3.1 SA-04(09) (HIGH; MOD) CMSRs v3.1 SA-09(02) (HIGH; MOD) CMSRs v3.1 SI-01 (HIGH; MOD) CRR v2016 CM:G2.Q2 CRR v2016 CM:G2.Q3 CRR v2016 CM:G2.Q4 EU GDPR Article 25(1) FedRAMP SA-4(9) FedRAMP SA-9(2) FedRAMP SI-1 ISO/IEC 27002:2013 14.1.1 ISO/IEC 27799:2016 14.1.1 MARS-E v2 SA-4(9) MARS-E v2 SA-9(2) MARS-E v2 SI-1 NIST Cybersecurity Framework v1.1 PR.IP-2 NIST SP 800-53 R4 PL-8(2)[S]{1} NIST SP 800-53 R4 SA-12(1)[S]{0} NIST SP 800-53 R4 SA-4(5)a[S]{1} NIST SP 800-53 R4 SA-4(9)[HM]{0} NY DOH SSP v3.1 PM-11b[M]-1 NY DOH SSP v3.1 SA-4(9)[M]-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CMMC Level 3 Subject to CMMC Level 4 Subject to CMMC Level 5 Subject to CRR V2016 Subject to NIST 800-171 Basic Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to Supplemental Requirements Subject to the EU GDPR
Level 2 Implementation:	Level 1 plus:

	Information security and privacy are addressed in all phases of the project management methodology. Organizations establish and appropriately protect a secure development environment for system development and integration efforts that cover the entire system development life cycle. The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of security requirements and controls in developed and acquired information systems. Organizations include business requirements for the availability of information systems when specifying security and privacy requirements. Where availability cannot be guaranteed using existing architectures, redundant components or architectures are considered along with the risks associated with implementing such redundancies. Specifications for the security and privacy control requirements include that automated controls be incorporated in the information system, supplemented by manual controls as needed. This is evidenced in a formal System Development Life Cycle (SDLC), which covers request initiation, requirements definition, analysis, communication, conflict detection and resolution, and evolution of requirements. The organization's security risk management process is integrated into all SDLC activities. System requirements for information security and processes for implementing security are integrated in the requirements definition phase. Also, in the SDLC initial planning or requirement stage, Data Classification and risk of the assets are assigned to ensure appropriate controls will be considered and the correct project team members are involved. The risk and classification activities require sign-off by management. Organizations developing software or systems perform thorough testing and verification during the development process. Independent acceptance testing is then undertaken (both for in-house and for outsourced developments) to ensure the system works as expected and only as expected. The extent of testing is in proportion to the importance and nature of the system. Information security roles and responsibilities are defined and documented throughout the system development life cycle. Commercial products sought to store and/or process covered information undergo a security assessment and/or security certification by a qualified assessor prior to implementation. (Not applicable to operating system software).
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC8.1 CMMC v1.0 RE.5.140-1 CMMC v1.0 RM.4.150-0 CMMC v1.0 SC.3.180-0 CMSRs v3.1 PM-07 (HIGH; MOD) CMSRs v3.1 SA-03 (HIGH) CMSRs v3.1 SA-03 (HIGH; MOD) CMSRs v3.1 SA-04 (HIGH; MOD) CMSRs v3.1 SA-08 (HIGH; MOD) CMSRs v3.1 SC-05 (HIGH; MOD) CRR v2016 CCM:G1.Q6 CSA CCM v3.0.1 GRM-01 EU GDPR Article 25(1) FedRAMP SA-3 FedRAMP SA-4 FedRAMP SA-8 FedRAMP SC-5 FFIEC IS v2016 A.6.27 HITRUST IRS Pub 1075 v2016 9.3.15.3 IRS Pub 1075 v2016 9.3.15.4 IRS Pub 1075 v2016 9.3.15.6 ISO/IEC 27001:2013 6.1.5 ISO/IEC 27002:2013 14.1.1 ISO/IEC 27002:2013 14.2.1 ISO/IEC 27002:2013 14.2.5

	ISO/IEC 27002:2013 14.2.6 ISO/IEC 27002:2013 14.2.8 ISO/IEC 27002:2013 17.2.1 ISO/IEC 27799:2016 14.1.1 ISO/IEC 27799:2016 14.2.1 ISO/IEC 27799:2016 14.2.5 ISO/IEC 27799:2016 14.2.6 ISO/IEC 27799:2016 14.2.8 ISO/IEC 27799:2016 17.2.1 MARS-E v2 PM-7 MARS-E v2 SA-3 MARS-E v2 SA-4 MARS-E v2 SA-8 MARS-E v2 SC-5 NIST 800-171 r2 3.13.2-0 NIST Cybersecurity Framework v1.1 PR.IP-2 NIST SP 800-53 R4 SA-11(3)a[S]{2} NIST SP 800-53 R4 SA-11(3)b[S]{0} NIST SP 800-53 R4 SA-15(5)[S]{0} NIST SP 800-53 R4 SA-15(6)[S]{0} NIST SP 800-53 R4 SA-18(1)[S]{1} NIST SP 800-53 R4 SA-18[S]{0} NIST SP 800-53 R4 SA-3a[HML]{0} NIST SP 800-53 R4 SA-3b[HML]{0} NIST SP 800-53 R4 SA-3d[HML]{0} NIST SP 800-53 R4 SA-4(6)b[S]{0} NIST SP 800-53 R4 SA-8[HM]{0} NIST SP 800-53 R4 SA-9(1)b[S]{0} NIST SP 800-53 R4 SC-38[S]{0} NIST SP 800-53 R4 SI-13(5)[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 CM-4(2)b[MN]-0 NY DOH SSP v3.1 CM-4(2)c[MN]-0 NY DOH SSP v3.1 SA-3b[M]-0 NY DOH SSP v3.1 SA-3d[M]-0 NY DOH SSP v3.1 SA-8[M]-0 PCI DSS v3.2.1 6.3 PMI DSP Framework PR.IP-1 SR v6.4 29b.1-0

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to CMMC Level 2 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Basic Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)

Level 3 Implementation:	Level 2 plus: The organization develops enterprise architecture with consideration for information security and privacy, and the resulting risk to organizational operations, organizational assets, individuals, and other organizations. The organization: 1. Develops an information security architecture for the information system that: i. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; ii. Describes how the information security architecture is integrated into, and supports, the enterprise architecture; and iii. Describes any information security assumptions about, and dependencies on, external services. 2. Reviews and updates (as necessary) the information security and privacy architecture whenever changes are made to the enterprise architecture; and 3. Ensures that planned information security and privacy architecture changes are reflected in the security plan and organizational procurements/acquisitions. The organization includes security functional, strength and assurance requirements; security-related documentation requirements; and developmental and evaluation-related assurance requirements in information system acquisition contracts based on applicable laws, policies, standards, guidelines and business needs. The organization requires the developer of the information system, system component, or information system service to provide: 1. a description of the functional properties of the security and privacy controls to be employed; and 2. design and implementation information for the security and privacy controls to be employed that includes: security-and privacy-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces and high-level design documentation at sufficient detail to prove the security and privacy control implementation. The organization documents all existing outsourced information services and conducts an organizational assessment of risk prior to the acquisition or outsourcing of information services.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC5.2 CMMC v1.0 CA.2.157-2 CMSRs v3.1 AR-07 (HIGH; MOD) CMSRs v3.1 PL-08 (HIGH; MOD) CMSRs v3.1 PM-07 (HIGH; MOD) CMSRs v3.1 SA-04 (HIGH; MOD) CMSRs v3.1 SA-04(01) (HIGH; MOD) CMSRs v3.1 SA-04(02) (HIGH; MOD) CMSRs v3.1 SA-09 (HIGH; MOD) CMSRs v3.1 SA-15 (HIGH; MOD) CMSRs v3.1 SA-17 (HIGH) EU GDPR Article 25(1) FedRAMP PE-14 FedRAMP SA-4 FedRAMP SA-4(1) FedRAMP SA-4(2) FedRAMP SA-9(1) IRS Pub 1075 v2016 9.3.15.4 IRS Pub 1075 v2016 Exhibit 10 MARS-E v2 AR-7 MARS-E v2 PM-7 MARS-E v2 SA-4

	MARS-E v2 SA-4(1) MARS-E v2 SA-4(2) MARS-E v2 SA-9(1) NIST 800-171 r2 3.12.4-2 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 PR.IP-2 NIST SP 800-53 R4 PL-8(1)b[S]{0} NIST SP 800-53 R4 PL-8a[HM]{1} NIST SP 800-53 R4 PL-8a[HM]{3} NIST SP 800-53 R4 PL-8c[HM]{0} NIST SP 800-53 R4 PM-7[HML]{0} NIST SP 800-53 R4 SA-12(2)[S]{0} NIST SP 800-53 R4 SA-15b[H]{0} NIST SP 800-53 R4 SA-17(1)[S]{0} NIST SP 800-53 R4 SA-20[S]{1} NIST SP 800-53 R4 SA-4(1)[HM]{0} NIST SP 800-53 R4 SA-4(2)[HM]{0} NIST SP 800-53 R4 SA-9(1)a[S]{0} NIST SP 800-53 R4 SI-12[HML]{3} NY DOH SSP v3.1 PL-8a[M]-0 NY DOH SSP v3.1 PL-8a2[M]-0 NY DOH SSP v3.1 PL-8a3[M]-0 NY DOH SSP v3.1 PL-8b[M]-0 NY DOH SSP v3.1 PL-8c[M]-0 NY DOH SSP v3.1 PM-7[M]-0 NY DOH SSP v3.1 SA-4(1)[M]-0 NY DOH SSP v3.1 SA-9(1).IS1[M]-0 NY DOH SSP v3.1 SA-9(1).IS2[M]-0 NY DOH SSP v3.1 SA-9(1)a[MN]-0

Level CMMC Implementation Requirements

Level CMMC Implementation:	The organization designs network and system security capabilities to leverage, integrate, and share Indicators of Compromise (IoC).

Level CMS Implementation Requirements

Level CMS Implementation:	The organization manages the information system using a formally defined and documented system development life cycle (SDLC) process that incorporates information security control considerations. The organization requires that contracts include the standard CMS information security and privacy contract language. The organization: 1. Requires the developer of the information system, system component, or information system service to follow a documented development process that: i. Explicitly addresses security requirements; ii. Identifies the standards and tools used in the development process; iii. Documents the specific tool options and tool configurations used in the development process; and iv. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and 2. Reviews the development process, standards, tools, and tool options/configurations at least every three years to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy all applicable System Acquisition (SA) and Configuration Management (CM) security controls. The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:

	1. Is consistent with and supportive of the organization's security architecture, which is established within, and is an integrated part of, the organization's enterprise architecture; 2. Accurately and completely describes the required security functionality, and the allocation of security controls, among physical and logical components; and 3. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The organization reviews and updates the information security architecture every 365 days or when a significant change occurs to the enterprise architecture and ensures that planned information security architecture changes are reflected in the security plan and organizational procurements and acquisitions. The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	Whenever information systems contain FTI, the agency includes security requirements (e.g., the capacity to block information to contractors when they are not authorized to access FTI) and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk. The contract for the acquisition must contain IRS Pub 1075 Exhibit 7 (E.7) language. Agencies using a consolidated data center must implement appropriate controls to ensure the protection of FTI, including a Service Level Agreement (SLA) between the agency authorized to receive FTI and the data center. The agency documents online and architectural adjustments that occur during the life cycle of a data warehouse and ensures that FTI is always secured from unauthorized access or disclosure. For critical online resources, redundant systems in a data warehouse are employed with automatic failover capability.

Level HIX Implementation Requirements

Level HIX Implementation:	Each contract and Statement of Work (SOW) that contain personally identifiable information (PII) must include language requiring adherence security and privacy policies and standards set by the organization consistent with 45 CFR 155.260(b), define security roles and responsibilities, and receive approval from the system owner. Acquisition contracts include a requirement that providers of defined external information systems identify the location of information systems that receive, process, store, or transmit information.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that contains organization-defined level of detail.

	The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs: (i) security functional requirements; (ii) security strength requirements; (iii) security assurance requirements; (iv) security-related documentation requirements; (v) requirements for protecting security-related documentation; (vi) description of the information system development environment and environment in which the system is intended to operate; and (vii) acceptance criteria. The organization requires the developer of the information system, system component, or information system service to follow a documented development process that (i) explicitly addresses security requirements; (ii) identifies the standards and tools used in the development process; (iii) documents the specific tool options and tool configurations used in the development process; and (iv) documents, manages, and ensures the integrity of changes to the process and/or tools used in development. The organization reviews the development process, standards, tools, and tool options/configurations within every 365 days to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy all applicable System Acquisition (SA) and Configuration Management (CM) security controls. The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: (i) security-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces; (ii) source code and hardware schematics; and (iii) high-level design documentation at sufficient detail to prove the security control implementation. The organization obtains administrator documentation for the information system, system component, or information system service that describes (i) secure configuration, installation, and operation of the system, component, or service; (ii) effective use and maintenance of security functions/mechanisms; and (iii) known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions. The organization obtains user documentation for the information system, system component, or information system service that describes (i) user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; (ii) methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and (iii) user responsibilities in maintaining the security of the system, component, or service. The information system must follow system security engineering principles consistent with (i) the information security steps of the CMS eXpedited Life Cycle (XLC) to incorporate information security control considerations; (ii) the information system architecture defined within the Technical Reference Architecture (TRA); and (iii) the Technical Review Board (TRB) processes defined by CMS.

Objective Name: 10.02 Correct Processing in Applications

Control Objective:	To ensure the prevention of errors, loss, unauthorized modification or misuse of information in applications, controls shall be designed into applications, including user developed applications to ensure correct processing. These controls shall include the validation of input data, internal processing and output data.

Control Reference: 10.b Input Data Validation

Control Specification:	Data input to applications and databases shall be validated to ensure that this data is correct and appropriate. *Required for HITRUST Certification CSF v9.6
Factor Type:	System
Topics:	Policies and Procedures; Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to FTC Red Flags Rule Subject to Joint Commission Accreditation Subject to NIST SP 800-53 R4 (Supplemental) Subject to Supplemental Requirements
Level 1 Implementation:	For organizations doing system development (e.g., applications, databases), checks are applied to the input of business transactions, standing data, and parameter tables - and minimally for covered information. The organization develops applications based on secure coding guidelines to prevent common coding vulnerabilities in software development processes including, but not limited to: 1. injection flaws, particularly SQL injection (validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.); 2. buffer overflow (validate buffer boundaries and truncate input strings); 3. insecure cryptographic storage (prevent cryptographic flaws); 4. insecure communications (properly encrypt all authenticated and sensitive communications); 5. improper error handling (do not leak information via error messages); 6. broken authentication/sessions (prevent unauthorized individuals from compromising legitimate account credentials, keys or session tokens that would otherwise enable an intruder to assume the identity of an authorized user). For web applications and application interfaces (internal or external), this also includes but is not limited to: 1. cross-site scripting (XSS) (validate all parameters before inclusion, utilize context-sensitive escaping, etc.); 2. improper access control, such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access functions (properly authenticate users and sanitize input; do not expose internal object references to users); 3. cross-site request forgery (CSRF) (do not reply on authorization credentials and tokens automatically submitted by browsers); Web-based applications are checked for the most current OWASP top 10 input-validation-related vulnerabilities.

	Alternatively, the inclusion of input validation checks in the testing methodology is in place and performed at least annually. Input validation testing can be manually performed. The following input validation procedures are performed: 1. dual input or other input checks, such as boundary checking or limiting fields to specific ranges of input data, to detect the following errors: i. out-of-range values; ii. invalid characters in data fields; iii. missing or incomplete data; iv. exceeding upper and lower data volume limits; v. unauthorized or inconsistent control data; 2. periodic review of the content of key fields or data files to confirm their validity and integrity; 3. procedures for responding to validation errors; 4. procedures for testing the plausibility of the input data; 5. verifying the identity of an individual opening or updating an account; 6. defining the responsibilities of all personnel involved in the data input process; and 7. creating a log of the activities involved in the data input process (see 9.aa).
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(3) 1 TAC § 390.2(a)(4)(A)(xi) CIS CSC v7.1 18.7 CMSRs v3.1 SI-10 (HIGH; MOD) CRR v2016 CM:G2.Q5 CSA CCM v3.0.1 AIS-01 CSA CCM v3.0.1 AIS-03 EU GDPR Article 25(1) FedRAMP SI-10 IRS Pub 1075 v2016 9.3.17.7 MARS-E v2 SI-10 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.DS-6 NIST SP 800-53 R4 AC-24(1)[S]{0} NIST SP 800-53 R4 SI-10(1)a[S]{0} NIST SP 800-53 R4 SI-10(3)[S]{2} NIST SP 800-53 R4 SI-10(4)[S]{2} NIST SP 800-53 R4 SI-10(5)[S]{0} NIST SP 800-53 R4 SI-3(8)[S]{1} NIST SP 800-53 R4 SI-3(9)[S]{0} PCI DSS v3.2.1 6.5 PCI DSS v3.2.1 6.5.1 PCI DSS v3.2.1 6.5.10 PCI DSS v3.2.1 6.5.2 PCI DSS v3.2.1 6.5.3 PCI DSS v3.2.1 6.5.4 PCI DSS v3.2.1 6.5.5 PCI DSS v3.2.1 6.5.6 PCI DSS v3.2.1 6.5.7 PCI DSS v3.2.1 6.5.8 PCI DSS v3.2.1 6.5.9 PMI DSP Framework PR.DS-5 SR v6.4 29a.i-0 TJC IM.04.01.01, EP 1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Is the system(s) accessible from the Internet? Yes Number of interfaces to other systems 25 to 75 Number of transactions per day Greater than 85,000 Number of users of the system(s) Greater than 5,500
Level 2 Regulatory Factors:	Subject to 23 NYCRR 500 Subject to Banking Requirements

	Subject to CA Civil Code § 1798.81.5 Subject to FedRAMP Certification Subject to HIPAA Security Rule Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to Supplemental Requirements Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: Applications that store, process or transmit covered information undergo application vulnerability testing at least annually by a qualified party, with an emphasis on input validation controls. Application input validation testing is automated through use of tools or other non-manual methods. Additionally, the organization: 1. develops and documents system and information integrity policy and procedures; 2. disseminates the system and information integrity policy and procedures to appropriate areas within the organization; 3. assigns responsible parties within the organization to annually review system and information integrity policy and procedures; and 4. updates the system and information integrity policy and procedures when organizational review indicates updates are required. The information system checks the validity of organization-defined information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible. For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: 1. reviewing applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes; 2. installing an automated technical solution that detects and prevents web-based attacks (e.g., a web-application firewall) in front of public-facing web applications, to continually check all traffic. If a public-facing application is not web-based, the organization implements a network-based firewall specific to the application type. If the traffic to the public-facing application is encrypted, the device either sits behind the encryption or is capable of decrypting the traffic prior to analysis. For in-house developed software, the organization ensures that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Procedures, guidelines and standards for the development of applications are periodically reviewed, assessed and updated as necessary by the appointed senior-level information security official of the organization.
Level 2	1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(h)

Control Standard Mapping:	23 NYCRR 500.08(b) 45 CFR Part § 164.312(c)(1) HIPAA.SR-1 CIS CSC v7.1 18.2 CIS CSC v7.1 18.7 CMSRs v3.1 SI-01 (HIGH; MOD) CMSRs v3.1 SI-10 (HIGH; MOD) FedRAMP SI-1 FedRAMP SI-10 FFIEC IS v2016 A.6.27(e) FFIEC IS v2016 A.6.27(g) IRS Pub 1075 v2016 9.3.17.7 IRS Pub 1075 v2016 Exhibit 10 MARS-E v2 SI-1 MARS-E v2 SI-10 NIST Cybersecurity Framework v1.1 DE.CM-8 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST SP 800-53 R4 SI-10(2)[S]{0} NIST SP 800-53 R4 SI-10(3)[S]{1} NIST SP 800-53 R4 SI-10(4)[S]{1} NIST SP 800-53 R4 SI-10[HM]{0} NIST SP 800-53 R4 SI-4(11)[S]{0} NIST SP 800-53 R4 SI-4(18)[S]{1} NRS 603A.215.1 NY DOH SSP v3.1 SI-10.PII[M]-0 NY DOH SSP v3.1 SI-10[M]-0 NY DOH SSP v3.1 SI-4.IS1b[HML]-0 PCI DSS v3.2.1 6.6 SR v6.4 29a.3-0 SR v6.4 29b.3-0 TJC IM.04.01.01, EP 1

Level CIS Implementation Requirements

Level CIS Implementation:	For applications that rely on a database, the organization uses standard hardening configuration templates. All systems that are part of critical business processes should also be tested. The organization places application firewalls in front of its critical servers to verify and validate the traffic going to the server. Any unauthorized services or traffic are blocked, and an alert generated.

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	Web-enabled application software in a data warehouse: 1. Prohibits generic meta-characters in input data; 2. procedures to prevent structured query language (SQL) injection; 3. Protects any variable used in scripts to prevent direct OS command attacks; 4. Arranges to have all comments removed for any code passed to the browser; 5. Prevents users from seeing any debugging information on the client; and 6. Undergoes a check before production deployment to ensure that all sample, test, and unused files have been removed from the production system.

Control Reference: 10.c Control of Internal Processing

Control Specification:	Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
Factor Type:	System
Topics:	Documentation and Records; Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to Joint Commission Accreditation Subject to Texas Health and Safety Code
Level 1 Implementation:	For organizations doing system development (e.g., applications, databases), the design and implementation of applications ensure that the risks of processing failures leading to a loss of integrity are minimized. Data integrity controls address: 1. the use of add, modify, and delete functions to implement changes to data; 2. the procedures to prevent programs running in the wrong order or running after failure of prior processing (see 9.a); 3. the use of appropriate programs to recover from failures to ensure the correct processing of data; and 4. protection against attacks using buffer overruns/overflows. A checklist for validation checking is prepared, activities documented, and the results kept secure. The checks to be incorporated include the following and can be manual: 1. session or batch controls, to reconcile data file balances after transaction updates; 2. balancing controls, to check opening balances against previous closing balances, namely: i. run-to-run controls, ii. file update totals, and iii. program-to-program controls; 3. validation of system-generated input data (see 10.b); 4. checks on the integrity, authenticity or any other security feature of data or software downloaded, or uploaded, between central and remote computers; 5. hash totals of records and files; 6. checks to ensure that application programs are run at the correct time; 7. checks to ensure that programs are run in the correct order and terminate in case of a failure, and that further processing is halted until the problem is resolved; and 8. creating an automated log of the activities involved in the processing (see 9.aa).
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 21 CFR Part 11.10(f) AICPA 2017 CC8.1 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 DI-02 (HIGH; MOD) CMSRs v3.1 SI-10 (HIGH; MOD) CRR v2016 CCM:G2.Q5 CSA CCM v3.0.1 AIS-01 EU GDPR Article 25(1) FedRAMP SI-10 FFIEC IS v2016 A.6.27(e) FFIEC IS v2016 A.6.29 MARS-E v2 DI-2 MARS-E v2 SI-10 NIST Cybersecurity Framework v1.1 PR.DS-6 PMI DSP Framework PR.DS-5 TJC IM.04.01.01, EP 1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Is the system(s) accessible from the Internet? Yes Number of interfaces to other systems 25 to 75 Number of transactions per day Greater than 85,000 Number of users of the system(s) Greater than 5,500
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CMMC Level 1 Subject to CMMC Level 2 Subject to CMMC Level 5 Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to HIPAA Security Rule Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Basic Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: Applications undergo application vulnerability testing annually by a qualified party, focusing on the use of add, modify, and delete functions to implement changes to data, and attacks using buffer overruns/overflows. Automated validation checks are conducted at an organization-defined frequency but no less than monthly and/or after organization-defined security-relevant events, through use of tools or other non-manual methods to detect unauthorized changes to information, firmware and software. Information system flaws are identified, reported, and corrected. All appropriate information pertaining to the discovered flaws in the information system, including the cause of the flaws, mitigation activities, and lessons learned are collected. The organization performs an integrity check of software and information daily. The organization incorporates the detection of unauthorized security-relevant changes to the information system into the organization incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes. The information system provides notification of failed security verification tests. Automated validation checks are conducted at an organization-defined frequency but no less than monthly and/or after organization-defined security-relevant events automated through use of tools or other non-manual methods to detect unauthorized changes to information, firmware and software. The organization employs integrity verification tools to detect unauthorized, security-relevant configuration changes to software and information.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.312(c)(2) HIPAA.SR-0 AICPA 2017 CC6.8 AICPA 2017 CC7.1 CMMC v1.0 CM.5.074-0 CMMC v1.0 IR.2.093-2

	CMMC v1.0 SI.1.210-0 CMSRs v3.1 SI-02 (HIGH; MOD) CMSRs v3.1 SI-06 (HIGH) CMSRs v3.1 SI-07 (HIGH; MOD) CMSRs v3.1 SI-07(01) (HIGH; MOD) CMSRs v3.1 SI-07(02) (HIGH) CMSRs v3.1 SI-07(05) (HIGH) CMSRs v3.1 SI-07(07) (HIGH; MOD) CMSRs v3.1 SI-10 (HIGH; MOD) CRR v2016 CCM:G2.Q6 FedRAMP SI-10 FedRAMP SI-2 FedRAMP SI-7 FedRAMP SI-7(1) FedRAMP SI-7(7) FFIEC IS v2016 A.8.1(l) IRS Pub 1075 v2016 9.3.17.7 MARS-E v2 CM-6(3) MARS-E v2 SI-10 MARS-E v2 SI-2 MARS-E v2 SI-7(1) MARS-E v2 SI-7(7) MARS-E v2 SI-9 NIST 800-171 r2 3.14.1-0 NIST Cybersecurity Framework v1.1 DE.CM-8 NIST Cybersecurity Framework v1.1 ID.RA-1 NIST Cybersecurity Framework v1.1 PR.DS-6 NIST Cybersecurity Framework v1.1 PR.DS-8 NIST Cybersecurity Framework v1.1 RS.MI-3 NIST SP 800-53 R4 CM-3(5)[S]{2} NIST SP 800-53 R4 SA-18(1)[S]{2} NIST SP 800-53 R4 SI-2a[HML]{0} NIST SP 800-53 R4 SI-7(12)[S]{0} NIST SP 800-53 R4 SI-7(7)[HM]{0} NIST SP 800-53 R4 SI-7[HM]{0} NRS 603A.215.1 NY DOH SSP v3.1 IR-3.IS1[HM]-2 NY DOH SSP v3.1 RA-5c[M]-1 NY DOH SSP v3.1 RA-5d[M]-1 NY DOH SSP v3.1 RA-5e[M]-0 NY DOH SSP v3.1 SI-2.IS4[HML]-0 NY DOH SSP v3.1 SI-2a[M]-0 NY DOH SSP v3.1 SI-7(7)[M]-0 NY DOH SSP v3.1 SI-7[M]-0 PCI DSS v3.2.1 6.6 TJC IM.04.01.01, EP 1

Level CMS	Implementation Requirements
Level CMS Implementation:	The information system fails to a known secure state of all failures preserving the maximum amount of state information in failure. The information system verifies the correct operation of system security functions upon system startup and restart, upon command by a user with appropriate privilege, periodically on a monthly basis, provides notification of failed automated security tests, notifies system administration when anomalies are discovered, and shuts down, restarts or performs some other defined alternative action (defined in the applicable security plan) when anomalies are discovered. The information system automatically implements security safeguards (defined in the applicable security plan) when integrity violations are discovered, and automated tools provide notification upon the discovery of discrepancies during integrity verification.

Level Community Supplemental Reqs 02	Implementation Requirements
Level Community Supplemental Reqs 02 Implementation:	The organization incorporates domain name system (DNS) blackholing into its incident detection and response procedures, including (i) generating alerts to security personnel

	on queries to resolve blackholed domains; (ii) ensuring blackholing can be done quickly, as part of incident containment and prevention; and (iii) integrating with threat intelligence and other threat indicator sources to pre-emptively blackhole domains.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The information system verifies the correct operation of system security functions upon system startup and restart, upon command by a user with appropriate privilege, and periodically on a monthly basis; provides notification of failed automated security tests; notifies system administrators or security personnel when anomalies are discovered; and shuts down, restarts or performs some other defined alternative action when anomalies are discovered.

Level HIPAA Implementation Requirements

Level HIPAA Implementation:	Health information systems processing personal health information: 1. ensure that each subject of care can be uniquely identified within the system; 2. be capable of merging duplicate or multiple records if it is determined that multiple records for the same subject of care have been created unintentionally or during a medical emergency

Level Providers Implementation Requirements

Level Providers Implementation:	Health information systems processing personal health information: 1. ensure that each subject of care can be uniquely identified within the system; 2. be capable of merging duplicate or multiple records if it is determined that multiple records for the same subject of care have been created unintentionally or during a medical emergency.

Control Reference: 10.d Message Integrity

Control Specification:	Requirements for ensuring authenticity and protecting message integrity in applications shall be identified and controls implemented.
Factor Type:	System
Topics:	Cryptography

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to CMMC Level 3 Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to Joint Commission Accreditation Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental)

	Subject to NY OHIP Moderate-Plus Security Baseline Subject to Texas Health and Safety Code Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	The information system provides mechanisms to protect the authenticity of communications sessions. Cryptographic controls (see 10.f) are implemented to ensure message authentication and integrity for covered information applications. The system implements one of the following integrity protection algorithms: 1. HMAC-SHA-1; or 2. HMAC-MD5. See NIST SP 800-52 Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations for more information on implementing integrity checks for information transmissions.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMMC v1.0 SC.3.190-0 CMSRs v3.1 SC-08 (HIGH; MOD) CMSRs v3.1 SC-23 (HIGH; MOD) FedRAMP SC-23 IRS Pub 1075 v2016 9.3.16.14 IRS Pub 1075 v2016 9.3.16.8 ISO/IEC 27002:2013 10.1.1 ISO/IEC 27799:2016 10.1.1 MARS-E v2 SC-23 MARS-E v2 SC-8 NIST 800-171 r2 3.13.15-0 NIST Cybersecurity Framework v1.1 PR.DS-2 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.DS-6 NIST SP 800-53 R4 AC-12(1)b[S]{0} NIST SP 800-53 R4 SC-15(4)[S]{0} NIST SP 800-53 R4 SC-23(1)[S]{0} NIST SP 800-53 R4 SC-23(3)[S]{0} NIST SP 800-53 R4 SC-23[HM]{0} NY DOH SSP v3.1 SC-23[M]-0 OCR Guidance for Unsecured PHI (1)(ii) PMI DSP Framework PR.DS-5 TJC IM.02.01.03, EP 6

Control Reference: 10.e Output Data Validation

Control Specification:	Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.
Factor Type:	System
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems

Level 1 Regulatory Factors:	Subject to Joint Commission Accreditation Subject to NIST SP 800-53 R4 (Supplemental)
Level 1 Implementation:	For organizations doing system development (e.g., applications, databases), output validation is manually or automatically performed. Output validation includes: 1. plausibility checks to test whether the output data is reasonable; 2. reconciliation control counts to ensure processing of all data; 3. providing sufficient information for a reader (i.e., to ensure that the client/customer they are serving matches the information retrieved, or subsequent processing system to determine the accuracy, completeness, precision, and classification of the information); 4. procedures for responding to output validation tests; 5. defining the responsibilities of all personnel involved in the data output process; and 6. creating an automated log of activities in the data output validation process.
Level 1 Control Standard Mapping:	CSA CCM v3.0.1 AIS-01 CSA CCM v3.0.1 AIS-03 EU GDPR Article 25(1) ISO/IEC 27002:2013 14.2.5 ISO/IEC 27799:2016 14.2.5 NIST SP 800-53 R4 PE-5(2)b[S]{1} NIST SP 800-53 R4 SI-15[S]{0} TJC IM.04.01.01, EP 1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Is the system(s) accessible from the Internet? Yes Number of interfaces to other systems 25 to 75 Number of transactions per day Greater than 85,000 Number of users of the system(s) Greater than 5,500
Level 2 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Supplemental)
Level 2 Implementation:	Level 1 plus: Output validation checks are automated.
Level 2 Control Standard Mapping:	ISO/IEC 27002:2013 14.2.5 ISO/IEC 27799:2016 14.2.5 NIST SP 800-53 R4 PE-5(2)b[S]{2}

Objective Name: 10.03 Cryptographic Controls

Control Objective:	To protect the confidentiality, authenticity and integrity of information by cryptographic means. A policy shall be developed on the use of cryptographic controls. Key management should be in place to support the use of cryptographic techniques.

Control Reference: 10.f Policy on the Use of Cryptographic Controls

Control Specification:	A policy on the use of cryptographic controls for protection of information shall be developed and implemented and supported by formal procedures.

	*Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Communications and Transmissions; Cryptography; Media and Assets; Policies and Procedures that address the approach to key management, including methods to deal with the protection of cryptographic keys and the recovery

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to HIPAA Security Rule Subject to Joint Commission Accreditation Subject to NY OHIP Moderate-Plus Security Baseline Subject to Texas Health and Safety Code Subject to the State of Nevada Security of Personal Information Requirements
Level 1 Implementation:	The cryptographic policy addresses the use of encryption for protection of covered and/or confidential information transported by mobile or removable media, devices or across communication lines. Supporting cryptographic procedures address: 1. the required level of protection (e.g., the type and strength of the encryption algorithm required); and 2. specifications for the effective implementation throughout the organization (i.e., which solution is used for which business processes). The cryptographic policy is aligned with the organization's data protection and privacy policy (see 06.d)
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.312(a)(2)(iv) HIPAA.SR-1 AICPA 2017 CC6.7 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 SC-13 (HIGH; MOD) CSA CCM v3.0.1 EKM-03 FedRAMP SC-13 FFIEC IS v2016 A.6.30 IRS Pub 1075 v2016 9.3.16.9 ISO/IEC 27002:2013 10.1.1 ISO/IEC 27799:2016 10.1.1 MARS-E v2 SC-13 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.DS-2 NRS 603A.215.2.a NY DOH SSP v3.1 AC-19(5).IS.PII1[M]-0 OCR Guidance for Unsecured PHI (1) TJC IM.02.01.03, EP 2

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters

	Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements
Level 2 Implementation:	Level 1 plus: When implementing the organization's cryptographic policy and procedures, the regulations and national restrictions that apply to the use of cryptographic techniques in different parts of the world and to the issues of trans-border flow of encrypted information (see 06.f) are adhered to.
Level 2 Control Standard Mapping:	COBIT 5 DS5.8 COBIT 5 DSS05.03 CSA CCM v3.0.1 GRM-06 FFIEC IS v2016 A.6.30 ISO/IEC 27002:2013 10.1.1 ISO/IEC 27799:2016 10.1.1 NIST Cybersecurity Framework v1.1 ID.GV-3

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	SEs must have a process or procedure in place for confirming that devices and media have been encrypted successfully using at least one of the following, listed in preferred order: (i) automated policy enforcement; (ii) automated inventory system; or (iii) manual record keeping. If encryption is used as an access control mechanism, it must meet CMS approved (FIPS 140-2 compliant and a NIST validated module) encryption standards.

Level PCI Implementation Requirements

Level PCI Implementation:	When being assessed as a service provider, the organization maintains a documented description of the cryptographic architecture that includes: (i) details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date; (ii) description of the key usage for each key; and (iii) inventory of any hardware security modules (HSMs) and other secure cryptographic devices (SCDs) used for key management.

Level Title 21 CFR Part 11 Implementation Requirements

Level Title 21 CFR Part 11 Implementation:	Persons using electronic signatures, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, use on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures by following the preceding steps: 1. The certification is submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857; and 2. Persons using electronic signatures, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signers hand-written signature.

Control Reference: 10.g Key Management

Control Specification:	Key management shall be in place to support the organization's use of cryptographic techniques.
Factor Type:	Organizational
Topics:	Authentication; Cryptography; Physical and Facility Security; Requirements (Legal and Contractual); Services and Acquisitions

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to Joint Commission Accreditation Subject to Texas Health and Safety Code Subject to the State of Nevada Security of Personal Information Requirements
Level 1 Implementation:	All cryptographic keys are protected against modification, loss, and destruction. In addition, secret and private keys require protection against unauthorized disclosure. Cryptographic keys are limited to the fewest number of custodians necessary. Equipment used to generate, store and archive keys is physically protected, and encryption keys are stored separately from encrypted data. If manual clear-text key-management procedures are used, the organization splits knowledge and control of keys (e.g., requiring multiple individuals, knowing only their respective key, comprising the whole key). Keys are not stored in the Cloud (i.e., at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage are separated duties.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) AICPA 2017 CC6.1 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CSA CCM v3.0.1 EKM-01 CSA CCM v3.0.1 EKM-02 FFIEC IS v2016 A.6.30 ISO/IEC 27002:2013 10.1.2 ISO/IEC 27799:2016 10.1.2 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.DS-2 PMI DSP Framework PR.DS-2 TJC IM.02.01.03, EP 6

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	

Level 2 Regulatory Factors:	Subject to CMMC Level 3 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: A key management system is based on a formal set of standards, procedures, and secure methods for: 1. verifying user identity prior to generating new certificates or keys; 2. generating keys for different cryptographic systems and different applications; 3. generating and obtaining public key certificates; 4. distributing keys to intended users, including how keys are activated when received; 5. storing keys in the fewest possible locations, including how authorized users obtain access to keys; 6. changing or updating keys including rules on when keys are changed and how this will be done: i. as deemed necessary and recommended by the associated application; and ii. at least annually; 7. revoking keys, including how keys are withdrawn or deactivated (e.g., when keys have been compromised or suspected to have been compromised or when a user leaves an organization, in which case keys are also archived); 8. recovering keys that are lost or corrupted as part of business continuity management (e.g., for recovery of encrypted information); 9. archiving keys (e.g., for information archived or backed up); 10. destroying keys; and 11. logging and auditing of key management related activities. In order to reduce the likelihood of compromise, activation, and deactivation, dates for keys are defined so that the keys can only be used for a limited period of time. This period of time is dependent on the circumstances under which the cryptographic control is being used, and the perceived risk, however the period of time cannot exceed one year. The organization prevents the unauthorized substitution of keys. Cryptographic key custodians are required to sign a form stating they understand and accept their key custodian responsibilities. In addition to securely managing secret and private keys, the authenticity of public keys is also addressed. This authentication process is done using public key certificates issued by a certification authority, which is a recognized organization with suitable controls and procedures in place to provide the required degree of trust.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC6.1 CMMC v1.0 SC.3.187-0 CMSRs v3.1 SC-12 (HIGH; MOD) CMSRs v3.1 SC-12(01) (HIGH) CMSRs v3.1 SC-17 (HIGH; MOD) COBIT 5 DS5.8 COBIT 5 DSS05.03 CSA CCM v3.0.1 EKM-02

	FedRAMP SC-12 FedRAMP SC-12(2) FedRAMP SC-17 IRS Pub 1075 v2016 9.3.16.11 IRS Pub 1075 v2016 9.3.16.8 ISO/IEC 27002:2013 10.1.2 ISO/IEC 27799:2016 10.1.2 MARS-E v2 SC-12 MARS-E v2 SC-12(2) MARS-E v2 SC-17 NIST 800-171 r2 3.13.10-0 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.DS-2 NIST SP 800-53 R4 SC-12(1)[H]{0} NIST SP 800-53 R4 SC-17[HM]{0} NIST SP 800-53 R4 SC-23(5)[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 SC-12(1)[HN]-0 NY DOH SSP v3.1 SC-12(2).IS1[M]-0 NY DOH SSP v3.1 SC-12(2)[MN]-0 NY DOH SSP v3.1 SC-12[M]-0 NY DOH SSP v3.1 SC-17[M]-0 PCI DSS v3.2.1 3.5 PCI DSS v3.2.1 3.5.2 PCI DSS v3.2.1 3.5.4 PCI DSS v3.2.1 3.5.8 PCI DSS v3.2.1 3.6 PCI DSS v3.2.1 3.6.1 PCI DSS v3.2.1 3.6.2 PCI DSS v3.2.1 3.6.3 PCI DSS v3.2.1 3.6.4 PCI DSS v3.2.1 3.6.5 PCI DSS v3.2.1 3.6.7 PCI DSS v3.2.1 8.2.2 PMI DSP Framework PR.DS-2

Level CMS Implementation Requirements

Level CMS Implementation:	The organization maintains availability of information in the event of the loss of cryptographic keys by users. Mechanisms are employed to: 1. prohibit the use of encryption keys that are not recoverable by authorized personnel; 2. require senior management approval to authorize recovery of keys by other than the key owner; and 3. comply with approved cryptography standards specified in 10.f.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The organization produces, controls, and distributes asymmetric cryptographic keys using: 1. NSA-approved key management technology and processes; 2. approved PKI Class 3 certificates or prepositioned keying material; or 3. approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the users private key.

Level PCI Implementation Requirements

Level PCI Implementation:	Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: 1. Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data- encrypting key; 2. Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device); or

	3. As at least two (two) full-length key components or key shares, in accordance with an industry-accepted method.

Objective Name: 10.04 Security of System Files

Control Objective:	To ensure the security of system files, access to system files and program source code shall be controlled, and IT projects and support activities conducted in a secure manner.

Control Reference: 10.h Control of Operational Software

Control Specification:	There shall be procedures in place to control the installation of software on operational systems. *Required for HITRUST Certification CSF v9.6
Factor Type:	System
Topics:	Authorization; Documentation and Records; Maintenance; Monitoring; Services and Acquisitions; Third-parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to CMMC Level 3 Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline
Level 1 Implementation:	To minimize the risk of corruption to operational systems, the following procedures are implemented to control changes: 1. the updating of the operational software, applications, and program libraries are only performed by authorized administrators; and 2. operational systems can only hold approved programs or executable code (i.e., no development code or compilers). Vendor supplied software used in operational systems is maintained at a level supported by the supplier. The organization uses the latest version of web browsers on operational systems to take advantage of the latest security functions in the application. The organization maintains information systems according to a current baseline configuration and configure system security parameters to prevent misuse. The operating system has in place supporting technical controls such as antivirus, file integrity monitoring, host-based (personal) firewalls or port filtering tools, and logging as part of their baseline. Any decision to upgrade to a new release takes into account the business requirements for the change, and the security and privacy impacts of the release (e.g., the introduction of new security functionality or the number and severity of security problems affecting this version).

	If systems or system components in production are no longer supported by the developer, vendor, or manufacturer, the organization must show evidence of a formal migration plan approved by management to replace the system or system components. Rules for the migration of software from development to operational status are defined and documented by the organization hosting the affected application(s), including that development, test, and operational systems be separated (physically or virtually) to reduce the risks of unauthorized access or changes to the operational system.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 21 CFR Part 11.10(a) AICPA 2017 CC8.1 CIS CSC v7.1 18.3 CIS CSC v7.1 7.1 CIS CSC v7.1 9.4 CMMC v1.0 RM.3.147-0 CMSRs v3.1 CM-04 (HIGH) CMSRs v3.1 CM-06 (HIGH; MOD) CMSRs v3.1 CM-06(01) (HIGH) CMSRs v3.1 CM-06(02) (HIGH) CSA CCM v3.0.1 CCC-04 CSA CCM v3.0.1 IVS-07 FedRAMP CM-4 FedRAMP SC-7(12) IRS Pub 1075 v2016 9.3.15.10 IRS Pub 1075 v2016 9.3.5.4 IRS Pub 1075 v2016 9.3.5.6 IRS Pub 1075 v2016 9.4.18 ISO/IEC 27002:2013 12.5.1 ISO/IEC 27799:2016 12.5.1 MARS-E v2 CM-4 MARS-E v2 SA-22 MARS-E v2 SC-7(12) NIST Cybersecurity Framework v1.1 PR.IP-1 NIST Cybersecurity Framework v1.1 PR.IP-3 NIST SP 800-53 R4 SA-22(1)[S]{2} NIST SP 800-53 R4 SA-22a[S]{0} NY DOH SSP v3.1 SA-22a[MN]-0 NY DOH SSP v3.1 SC-7(12)[MN]-2 PCI DSS v3.2.1 2.2.4

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Is the scoped system(s) (on-premise or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? Yes Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CMMC Level 3 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline
Level 2 Implementation:	Level 1 plus: Applications and operating system software are only implemented after successful testing. The tests include tests on usability, security, and effects on other systems, and

	are carried out on separate systems. It is ensured that all corresponding program source libraries have been updated. A configuration control system is used to keep control of all implemented software as well as the system documentation. A rollback strategy is in place before changes are implemented. An audit log is maintained of all updates to operational program libraries. Previous versions of application software are retained as a contingency measure. Old versions of software are archived, together with all required information and parameters, procedures, configuration details, and supporting software for as long as the data is retained in archive or as dictated by the organization's data retention policy. Physical or logical access are only given to suppliers for support purposes when necessary, and with management approval. The supplier's activities are monitored. The organization prevents program execution in accordance with the list of unauthorized (blacklisted) software programs and rules authorizing the terms and conditions of software program usage. The organization: 1. identifies unauthorized (blacklisted) software on the information system, including servers, workstations and laptops; 2. employs an allow-all, deny-by-exception policy to prohibit the execution of known unauthorized (blacklisted) software on the information system; and 3. reviews and updates the list of unauthorized (blacklisted) software periodically, but no less than annually.
Level 2 Control Standard Mapping:	21 CFR Part 11.10(a) CMMC v1.0 CA.3.162-0 CMMC v1.0 CM.3.068-2 CMMC v1.0 CM.3.069-1 CMSRs v3.1 CM-02(03) (HIGH; MOD) CMSRs v3.1 CM-03 (HIGH; MOD) CMSRs v3.1 CM-03(02) (HIGH; MOD) CMSRs v3.1 CM-07(02) (HIGH; MOD) CMSRs v3.1 CM-07(05) (HIGH) FedRAMP CM-2(3) FedRAMP CM-7(5) FFIEC IS v2016 A.6.17 ISO/IEC 27002:2013 12.1.14 ISO/IEC 27002:2013 12.5.1 ISO/IEC 27799:2016 12.5.1 MARS-E v2 CM-2(3) MARS-E v2 CM-3 MARS-E v2 CM-3(2) NIST 800-171 r2 3.4.7-2 NIST 800-171 r2 3.4.8-1 NIST Cybersecurity Framework v1.1 PR.DS-7 NIST Cybersecurity Framework v1.1 PR.IP-1 NIST Cybersecurity Framework v1.1 PR.IP-3 NIST SP 800-53 R4 CM-2(3)[HM]{0} NIST SP 800-53 R4 CM-7(2)[HM]{0} NIST SP 800-53 R4 CM-7(4)[M]{0} NIST SP 800-53 R4 SA-10(5)[S]{1} NY DOH SSP v3.1 CM-1.IS1[M]-3 NY DOH SSP v3.1 CM-2(3).IS1[M]-2 NY DOH SSP v3.1 CM-2(3)[M]-0 NY DOH SSP v3.1 CM-3(2)[M]-0 NY DOH SSP v3.1 CM-7(2)b[M]-0 NY DOH SSP v3.1 CM-7(4)a[M]-0 NY DOH SSP v3.1 CM-7(4)b[M]-0 NY DOH SSP v3.1 SA-11(5).PII[MN]-2 NY DOH SSP v3.1 SA-11(5)[MN]-2

Level CIS	Implementation Requirements
Level CIS Implementation:	The organization maintains an up-to-date list of authorized software that is required in the enterprise for any business purpose on any business system. The organization deploys application whitelisting technology that allows systems to run software only if it is authorized to execute (whitelisted) and prevents execution of all other software on the system. Unnecessary browser and email client plugins and/or add-on applications that are not absolutely necessary for the functionality of the application are uninstalled or disabled. Each plugin utilizes application/URL whitelisting and only allows the use of the application for pre-approved domains. The organization ensures that only authorized scripting languages are able to run in all web browsers and email clients.

Level Cloud Service Providers	Implementation Requirements
Level Cloud Service Providers Implementation:	Cloud service providers use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications. In addition, all structured and unstructured data are available to the organization (customer) and provided to them upon request in an industry-standard format (e.g., .doc, .xls, pdf, logs, and flat files).

Level CMMC	Implementation Requirements
Level CMMC Implementation:	The organization utilizes an exception process for non-whitelisted software that includes mitigation techniques.

Level CMS	Implementation Requirements
Level CMS Implementation:	The organization responds to unauthorized changes to information system and components by alerting responsible actors (person, organization), restoring to the approved configuration, and halting system processing as warranted.

Level FTI Custodians	Implementation Requirements
Level FTI Custodians Implementation:	To access FTI using a web browser, the agency must determine the business use of Java and approve the use of Java if is required for core business functions.

Level NYDOH	Implementation Requirements
Level NYDOH Implementation:	The organization takes the following actions when unauthorized components and/or provisioned configurations are detected: (i) Disable access to the identified component; (ii) Disable the identified component's network access; (iii) Isolate the identified component; and (iv) Notify the responsible actor (i.e., person/organization-defined in security plan). The information system prohibits user installation of software without explicit privileged status.

	The organization provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

Control Reference: 10.i Protection of System Test Data

Control Specification:	Test data shall be selected carefully and protected and controlled in non-production environments.
Factor Type:	System
Topics:	Authorization; Data Loss Prevention; Documentation and Records; User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to Community Supplemental Requirements 002 Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline
Level 1 Implementation:	The use of operational databases containing covered information for non-production (e.g., testing) purposes is avoided. If covered, or otherwise sensitive, information must be used for testing purposes, all sensitive details and content are removed or modified beyond recognition (e.g., de-identified) before use. The following requirements are applied to protect data, when used for testing purposes: 1. the access control procedures, which apply to operational application systems, also apply to test application systems (see 1.0); 2. there is formal management authorization for instances where operational information is copied to a non-production application system; and 3. operational information and test accounts are erased from a test application system immediately after the testing is complete.
Level 1 Control Standard Mapping:	CSA CCM v3.0.1 DSI-05 CSR002 v2018 12.2-0-0 CSR002 v2018 12.3-0-0 IRS Pub 1075 v2016 9.4.6 ISO/IEC 27002:2013 14.3.1 ISO/IEC 27799:2016 14.3.1 NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.AC-2 NIST Cybersecurity Framework v1.1 PR.AC-3 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.AC-5 NIST SP 800-53 R4 SA-15(9)[S]{0} NY DOH SSP v3.1 SA-15(9)[M]-0 PCI DSS v3.2.1 6.4

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Is the system(s) accessible from the Internet? Yes Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500

Level 2 Regulatory Factors:	Subject to CA Civil Code § 1798.81.5 Subject to Community Supplemental Requirements 002 Subject to IRS Pub 1075 Compliance
Level 2 Implementation:	Level 1 plus: The following requirements are applied to protect operational data, when used for testing purposes: 1. security controls are equally applied to non-production environments as production environments; 2. all instances where covered information is used in non-production environments must be documented; and 3. the copying, use and erasure of operational information are logged to provide an audit trail. Personnel developing and testing system code do not have access to production libraries.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CSR002 v2018 12.1-0-0 IRS Pub 1075 v2016 9.4.6 ISO/IEC 27002:2013 14.3.1 ISO/IEC 27799:2016 14.3.1 NIST Cybersecurity Framework v1.1 PR.AC-1 NIST Cybersecurity Framework v1.1 PR.AC-2 NIST Cybersecurity Framework v1.1 PR.AC-3 NIST Cybersecurity Framework v1.1 PR.AC-4 NIST Cybersecurity Framework v1.1 PR.AC-5 NIST Cybersecurity Framework v1.1 PR.PT-1 NIST Cybersecurity Framework v1.1 PR.PT-3

Level FTI Custodians Implementation Requirements

Level FTI Custodians Implementation:	The agency avoids (limits) the use of live FTI-primarily unmodified, non-sanitized data extracted from taxpayer files that identifies specific individual or corporate taxpayers and includes taxpayer information or tax return information-in pre-production (e.g., test environments) and is not authorized unless specifically approved by the Office of Safeguards through the submission of a Data Testing Request (DTR) form. The DTR must provide a detailed explanation of the safeguards in place to protect the data and the necessity for using live data during testing. The organization revises its Need and Use Justification to cover this use of IRS data if not already addressed. For one-time testing efforts, the agency detects the FTI from systems and databases upon completion of testing efforts and electronically clears the hard drive(s) of the test systems prior to repurposing the system for other agency testing efforts. The agency agrees with the Office of Safeguards to a specific duration for ongoing test activities.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	Production data may be used for testing, only if a business case is documented and approved, in writing, by the information owner and the following controls are applied: all security measures, including but not limited to access controls, system configurations, and logging requirements for the production data are applied to the test environment, and the data is deleted as soon as the testing is completed; or sensitive data is masked or overwritten with fictional information.

Control Reference: 10.j Access Control to Program Source Code

Control Specification:	Access to program source code shall be restricted.
Factor Type:	System
Topics:	Authorization; Policies and Procedures; Risk Management and Assessments; Services and Acquisitions; User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Supplemental)
Level 1 Implementation:	Access to program source code (code written by programmers, which is compiled and linked to create executables) and associated items (such as designs, specifications, verification plans and validation plans) is strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes. An organization will not have access to source code for the majority of purchased software applications, and this requirement does not apply.
Level 1 Control Standard Mapping:	CMSRs v3.1 CM-05 (HIGH; MOD) CMSRs v3.1 CM-07 (HIGH; MOD) CSA CCM v3.0.1 IAM-06 CSA CCM v3.0.1 IAM-09 FedRAMP CM-5 FedRAMP CM-7 ISO/IEC 27002:2013 9.4.5 ISO/IEC 27799:2016 9.4.5 MARS-E v2 CM-5 MARS-E v2 CM-7 NIST Cybersecurity Framework v1.1 PR.DS-5 NIST Cybersecurity Framework v1.1 PR.PT-3 NIST SP 800-53 R4 AC-3(5)[S]{1} NIST SP 800-53 R4 SA-10(6)[S]{1} NIST SP 800-53 R4 SA-15(2)[S]{0}

Level 2 Implementation Requirements

Level 2 Organizational Factors:	
Level 2 System Factors:	Is the system(s) accessible from the Internet? Yes Number of transactions per day 6,750 to 85,000 Number of users of the system(s) 500 to 5,500
Level 2 Regulatory Factors:	Subject to FedRAMP Certification Subject to NIST SP 800-53 R4 (Supplemental)
Level 2 Implementation:	Level 1 plus: Program source code is stored in a central location, specifically in program source libraries. The following requirements are implemented (see 1.0) to control access to such program source libraries in order to reduce the potential for corruption of computer programs: 1. program source libraries are not held in operational systems; 2. the program source code and the program source libraries are managed according to established procedures;

	3. access to program source libraries is strictly limited to that which is needed to perform a job function; 4. the updating of program source libraries and associated items, and the issuing of program sources to programmers only performed after appropriate authorization has been received; 5. program listings are held in a secure environment (see 9.r); 6. an audit log is maintained of all accesses to program source libraries; and 7. maintenance and copying of program source libraries are subject to strict change control procedures (see 10.k).
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 AC-06 (HIGH; MOD) CMSRs v3.1 CM-05 (HIGH; MOD) CSA CCM v3.0.1 IAM-06 FedRAMP AC-6 FedRAMP CM-5 IRS Pub 1075 v2016 9.3.1.6 IRS Pub 1075 v2016 9.3.5.5 ISO/IEC 27002:2013 9.4.5 ISO/IEC 27799:2016 9.4.5 MARS-E v2 AC-6 MARS-E v2 CM-5 NIST Cybersecurity Framework v1.1 PR.PT-3 NIST SP 800-53 R4 AC-3(5)[S]{2} NIST SP 800-53 R4 CM-5(6)[S]{1}

Objective Name: 10.05 Security In Development and Support Processes

Control Objective:	To ensure the security of application system software and information through the development process, project and support environments shall be strictly controlled.

Control Reference: 10.k Change Control Procedures

Control Specification:	The implementation of changes, including patches, service packs, and other updates and modifications, shall be controlled by the use of formal change control procedures. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Documentation and Records; IT Organization and Management Roles and Responsibilities; Requirements (Legal and Contractual)

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline
Level 1 Implementation:	Project and support environments are strictly controlled. Managers responsible for application systems are also responsible for the security of the project or support

	environment. They ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment. The organization manages changes to mobile device operating systems, patch levels, and/or applications through a formal change management process.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 CM-03 (HIGH; MOD) CRR v2016 CCM:G1.Q1 CSA CCM v3.0.1 MOS-15 FedRAMP CM-3 IRS Pub 1075 v2016 9.3.5.3 ISO/IEC 27001:2013 8.1 ISO/IEC 27002:2013 14.2.3 ISO/IEC 27002:2013 14.2.6 ISO/IEC 27799:2016 14.2.3 ISO/IEC 27799:2016 14.2.6 MARS-E v2 CM-3 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 PR.IP-3 NIST SP 800-53 R4 CM-3(4)[S]{0} NIST SP 800-53 R4 CM-3b[HM]{2} NIST SP 800-53 R4 CM-4[HML]{0} NY DOH SSP v3.1 CM-3b[M]-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to CMMC Level 2 Subject to EHNAC Accreditation Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance
Level 2 Implementation:	Level 1 plus: A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance is developed. Configuration management policy/procedures are reviewed/updated annually. The organization develops, documents, and implements a configuration management plan for the information system that: 1. addresses roles, responsibilities, and configuration management processes and procedures;

2. defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and
3. establishes a process for identifying configuration items throughout the system development life cycle, and for managing the configuration of the configuration items.
4. protects the configuration management plan from unauthorized disclosure and modification.

Formal change control procedures are documented and enforced in order to minimize the corruption of information systems. Introduction of new systems and major changes to existing systems follow a formal process of documentation, specification, testing, quality control, and managed implementation.

This process includes a risk assessment, analysis of the security and privacy impacts of changes, and specification of security controls needed. This process also ensures that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained.

Installation checklists are used to validate the configuration of servers, devices and appliances. In addition, vulnerability port scanning occurs on server and desktops and compares to a known effective baseline to ensure configuration meets minimum security standards. If a change that is not listed on the organization's approved baseline is discovered, an alert is generated and reviewed by the organization.

The change procedures minimally include:

1. ensuring changes are submitted by authorized users;
2. maintaining a record of agreed authorization levels;
3. reviewing controls and integrity procedures to ensure that they will not be compromised by the changes;
4. identifying all software, information, database entities, and hardware that require amendment;
5. obtaining formal approval for detailed proposals requesting changes before work commences;
6. documenting unit, system, and user acceptance testing procedures in an environment segregated from development and production;
7. ensuring all system components are tested and approved (operating system, utility, applications) prior to promotion to production;
8. documenting rollback procedures for failed changes;
9. ensuring authorized users accept changes prior to implementation based on the results on the completion of each change or testing of the changes;
10. ensuring that the system documentation set is updated, and that old documentation is archived or disposed of;
11. maintaining a version control for all software updates;
12. maintaining an audit trail of all change requests and approvals;
13. testing for mobile device, operating system, and application compatibility issues via a documented application validation process; and
14. ensuring that operating documentation (see 9.a) and user procedures are changed as necessary to remain appropriate.

If development is outsourced, change control procedures to address security are included in the contract(s). Automated updates are not used on critical systems, as some updates may cause critical applications to fail.

The organization requires the developer of the information system, system component, or information system service to track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel or roles.

Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMMC v1.0 CM.2.065-0 CMSRs v3.1 CM-01 (HIGH; MOD) CMSRs v3.1 CM-02(02) (HIGH) CMSRs v3.1 CM-03 (HIGH; MOD) CMSRs v3.1 CM-03(01) (HIGH) CMSRs v3.1 CM-03(02) (HIGH; MOD) CMSRs v3.1 CM-04 (HIGH; MOD) CMSRs v3.1 CM-04(01) (HIGH; MOD) CMSRs v3.1 CM-05 (HIGH; MOD) CMSRs v3.1 CM-05(01) (HIGH) CMSRs v3.1 CM-05(03) (HIGH) CMSRs v3.1 CM-06 (HIGH; MOD) CMSRs v3.1 CM-09 (HIGH; MOD) CMSRs v3.1 SA-10 (HIGH; MOD) CRR v2016 CCM:G1.Q1 CRR v2016 CCM:G1.Q4 CRR v2016 CCM:G1.Q6 CRR v2016 CCM:G2.Q1 CRR v2016 CCM:G2.Q2 CRR v2016 CCM:G2.Q3 CRR v2016 CCM:G2.Q4 CRR v2016 CCM:G2.Q7 CSA CCM v3.0.1 CCC-05 CSA CCM v3.0.1 MOS-07 FedRAMP CM-1 FedRAMP CM-3 FedRAMP CM-4 FedRAMP CM-5 FedRAMP CM-5(3) FedRAMP CM-5(5) FedRAMP CM-6 FedRAMP CM-9 FedRAMP SA-10 FFIEC IS v2016 A.6.11(a) FFIEC IS v2016 A.6.11(b) FFIEC IS v2016 A.6.11(c) FFIEC IS v2016 A.6.11(d) FFIEC IS v2016 A.6.11(e) FFIEC IS v2016 A.6.11(f) FFIEC IS v2016 A.6.11(g) FFIEC IS v2016 A.6.11(h) FFIEC IS v2016 A.6.11(i) FFIEC IS v2016 A.6.11(j) FFIEC IS v2016 A.6.11(k) FFIEC IS v2016 A.6.11(l) FFIEC IS v2016 A.6.11(m) FFIEC IS v2016 A.6.12 FFIEC IS v2016 A.6.15(d) FFIEC IS v2016 A.6.15(g) FFIEC IS v2016 A.6.15(h) FFIEC IS v2016 A.6.28(a) IRS Pub 1075 v2016 9.3.15.8 IRS Pub 1075 v2016 9.3.5.1 IRS Pub 1075 v2016 9.3.5.3 IRS Pub 1075 v2016 9.3.5.4 IRS Pub 1075 v2016 9.3.5.5 IRS Pub 1075 v2016 9.3.5.6 IRS Pub 1075 v2016 9.3.5.9 ISO/IEC 27002:2013 14.2.2 ISO/IEC 27002:2013 14.2.4 ISO/IEC 27002:2013 14.2.7 ISO/IEC 27799:2016 14.2.2 ISO/IEC 27799:2016 14.2.4 ISO/IEC 27799:2016 14.2.7 MARS-E v2 CM-1 MARS-E v2 CM-3 MARS-E v2 CM-3(2) MARS-E v2 CM-4 MARS-E v2 CM-4(1) MARS-E v2 CM-4(2) MARS-E v2 CM-5 MARS-E v2 CM-6 MARS-E v2 CM-9 MARS-E v2 SA-10

	NIST 800-171 r2 3.4.3-0 NIST Cybersecurity Framework v1.1 DE.CM-1 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 ID.RA-4 NIST Cybersecurity Framework v1.1 ID.RA-5 NIST Cybersecurity Framework v1.1 PR.AT-3 NIST Cybersecurity Framework v1.1 PR.IP-1 NIST Cybersecurity Framework v1.1 PR.IP-2 NIST Cybersecurity Framework v1.1 PR.IP-3 NIST Cybersecurity Framework v1.1 PR.PT-3 NIST SP 800-53 R4 CM-3a[HM]{0} NIST SP 800-53 R4 CM-3g[HM]{1} NIST SP 800-53 R4 CM-9[HM]{0} NIST SP 800-53 R4 RA-5b[HML]{2} NIST SP 800-53 R4 SA-10(2)[S]{0} NIST SP 800-53 R4 SA-12(15)[S]{0} NIST SP 800-53 R4 SA-12(7)[S]{0} NIST SP 800-53 R4 SA-15(11)[S]{0} NRS 603A.215.1 NY DOH SSP v3.1 CM-1.IS1[M]-1 NY DOH SSP v3.1 CM-1a[M]-0 NY DOH SSP v3.1 CM-1a1[M]-0 NY DOH SSP v3.1 CM-3c[M]-0 NY DOH SSP v3.1 CM-9[M]-0 NY DOH SSP v3.1 CM-9a[M]-0 NY DOH SSP v3.1 CM-9b[M]-0 NY DOH SSP v3.1 CM-9c[M]-0 NY DOH SSP v3.1 CM-9d[M]-0 NY DOH SSP v3.1 CM-9e[M]-0 PCI DSS v3.2.1 6.4

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to Banking Requirements Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 2 Subject to CMMC Level 3 Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Basic Level Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Supplemental Requirements Subject to the CMS Minimum Security Requirements (High)

Level 3 Implementation:	Level 2 plus: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system. The organization reviews and updates the baseline configuration of the information system: 1. at least once every six months; 2. when required due to critical security patches, upgrades and emergency changes (e.g., unscheduled changes, system crashes, replacement of critical hardware components), major system changes/upgrades; i. as an integral part of information system component installations, ii. upgrades, and iii. supporting baseline configuration documentation reflects ongoing implementation of operational configuration baseline updates, either directly or by policy. The organization: 1. establishes and documents mandatory configuration settings for information technology products employed within the information system using the latest security configuration baselines established by an authoritative source, e.g., DHS, U.S. Government Configuration Baselines (USGCB), and the National Checklist Program (NCP) defined by NIST SP 800-70 Rev. 2, that reflect the most restrictive mode consistent with operational requirements; 2. identifies, documents, and approves exceptions from the mandatory established configuration settings for individual components within the information system based on explicit operational requirements; and 3. monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings. The organization employs automated mechanisms to respond to unauthorized changes to network and system security-related configuration settings. The information system enforces access restrictions and supports auditing of the enforcement actions. The integrity of all virtual machine images is ensured at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to the business owner(s) and/or customer(s) through electronic methods (e.g., portals or alerts).
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC4.1 AICPA 2017 CC6.8 AICPA 2017 CC7.1 AICPA 2017 CC8.1 CIS CSC v7.1 11.3 CIS CSC v7.1 5.1 CIS CSC v7.1 5.2 CIS CSC v7.1 5.4 CMMC v1.0 CM.2.061-1 CMMC v1.0 CM.2.064-0 CMMC v1.0 CM.3.067-0 CMSRs v3.1 CM-02 (HIGH; MOD) CMSRs v3.1 CM-02(01) (HIGH; MOD) CMSRs v3.1 CM-02(02) (HIGH) CMSRs v3.1 CM-02(03) (HIGH; MOD) CMSRs v3.1 CM-05(02) (HIGH)

CMSRs v3.1 CM-06 (HIGH; MOD)
CMSRs v3.1 CM-06(01) (HIGH)
CMSRs v3.1 CM-06(02) (HIGH)
CRR v2016 CCM:G3.Q1
CRR v2016 CCM:G3.Q2
CSA CCM v3.0.1 IVS-02
FedRAMP CM-2
FedRAMP CM-2(1)
FedRAMP CM-6(1)
FFIEC IS v2016 A.6.12
FFIEC IS v2016 A.6.14
IRS Pub 1075 v2016 9.3.5.2
IRS Pub 1075 v2016 9.3.5.6
IRS Pub 1075 v2016 9.4.11
IRS Pub 1075 v2016 9.4.13
IRS Pub 1075 v2016 9.4.14
IRS Pub 1075 v2016 9.4.15
IRS Pub 1075 v2016 9.4.16
IRS Pub 1075 v2016 9.4.17
IRS Pub 1075 v2016 9.4.18
IRS Pub 1075 v2016 9.4.3
IRS Pub 1075 v2016 9.4.5
IRS Pub 1075 v2016 9.4.8
IRS Pub 1075 v2016 9.4.9
IRS Pub 1075 v2016 Exhibit 10
MARS-E v2 CM-2
MARS-E v2 CM-2(1)
MARS-E v2 CM-6
MARS-E v2 CM-6(1)
NIST 800-171 r2 3.4.1-1
NIST 800-171 r2 3.4.2-0
NIST 800-171 r2 3.4.5-0
NIST Cybersecurity Framework v1.1 DE.CM-1
NIST Cybersecurity Framework v1.1 DE.CM-7
NIST Cybersecurity Framework v1.1 PR.IP-1
NIST Cybersecurity Framework v1.1 PR.IP-3
NIST SP 800-53 R4 CM-2(1)[HM]{0}
NIST SP 800-53 R4 CM-2[HML]{0}
NIST SP 800-53 R4 CM-3(3)[S]{0}
NIST SP 800-53 R4 CM-3(5)[S]{1}
NIST SP 800-53 R4 CM-3f[HM]{0}
NIST SP 800-53 R4 CM-3g[HM]{2}
NIST SP 800-53 R4 CM-6(1)[H]{0}
NIST SP 800-53 R4 CM-6(2)[H]{1}
NIST SP 800-53 R4 CM-6[HML]{0}
NIST SP 800-53 R4 CM-8(6)[S]{1}
NIST SP 800-53 R4 SA-10(4)[S]{1}
NIST SP 800-53 R4 SA-4(5)b[S]{0}
NIST SP 800-53 R4 SC-34(1)[S]{0}
NIST SP 800-53 R4 SC-34[S]{0}
NIST SP 800-53 R4 SI-14[S]{0}
NY DOH SSP v3.1 CM-2(1)a[M]-0
NY DOH SSP v3.1 CM-2(1)b[M]-0
NY DOH SSP v3.1 CM-2(1)c1[M]-0
NY DOH SSP v3.1 CM-2(1)c2[M]-0
NY DOH SSP v3.1 CM-2(1)c3[M]-0
NY DOH SSP v3.1 CM-2(1)d[M]-0
NY DOH SSP v3.1 CM-2(3).IS1[M]-1
NY DOH SSP v3.1 CM-2.IS2[M]-0
NY DOH SSP v3.1 CM-2.IS3[M]-0
NY DOH SSP v3.1 CM-2[M]-0
NY DOH SSP v3.1 CM-3a[M]-0
NY DOH SSP v3.1 CM-3d[M]-1
NY DOH SSP v3.1 CM-5(2).IS1[M]-2
NY DOH SSP v3.1 CM-6(1).IS1[M]-0
NY DOH SSP v3.1 CM-6(1).IS2[M]-0
NY DOH SSP v3.1 CM-6(1)[HN]-0
NY DOH SSP v3.1 CM-6a[M]-0
NY DOH SSP v3.1 CM-6b[M]-0
NY DOH SSP v3.1 CM-6c[M]-0
NY DOH SSP v3.1 CM-6d[M]-0
SR v6.4 17.9-0
SR v6.4 6.1-0

Level CIS Implementation Requirements	
Level CIS Implementation:	The organization builds secure images for workstations, servers and other system types from their secure configuration baselines and uses these images to build all new systems it deploys. Any existing systems that must be rebuilt (e.g., due to compromise) are rebuilt from the organizations secure images. Regular updates or exceptions to these secure images are formally managed by the organizations change management processes.

Level CMS Implementation Requirements	
Level CMS Implementation:	HHS-specific minimum-security configurations are used for the following OS and Applications: HHS approved USGCB Windows Standards (e.g., Microsoft supported versions only), Blackberry Server - Websense; and for all other OS's and applications, and to resolve configuration conflicts among multiple security guidelines, the CMS hierarchy for implementing security configuration guidelines. The organization reviews information system changes weekly, and when unauthorized changes or unexpected levels of system performance are indicated. The information system prevents the installation of network and server software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization. The organization employs automated mechanisms to: 1. document proposed changes to the information system; 2. notify designated approval authorities and request change approval; 3. highlight approvals that have not been approved or disapproved in a timely manner; 4. prohibit change until designated approvals are received; 5. document all changes to the information system; and 6. notify identified stakeholders when approved changes to the information system are completed. The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice. The organization employs automated mechanisms to maintain up-to-date, complete, accurate, and readily available baseline configuration of the information system.

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation:	The organization employs automated mechanisms to maintain up-to-date, complete, accurate, and readily available baseline configurations of the information system. The service provider establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the federal government and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the Joint Authorization Board (JAB) and Authorizing Official (AO). The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.

	The information system prevents the installation of network, server and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization. If digital signatures/certificates are unavailable, alternative cryptographic integrity checks (hashes, self-signed certs, etc.) can be utilized. The service provider uses the Center for Internet Security guidelines (Level 1) to establish configuration settings or establishes its own configuration settings if United States Government Configuration Baseline (USGCB) is not available; and ensures that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available). The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.

Level FTI Custodians	Implementation Requirements
Level FTI Custodians Implementation:	All agency information systems used for receiving, processing, storing and transmitting FTI must be hardened (securely configured) using, when available for the specific technologies used, Safeguard Computer Security Evaluation Matrices (SCSEMs) publicly available on the Office of Safeguards IRS.gov website, keyword: safeguards program. This requirement includes, but is not limited to: 1. email servers and clients; 2. integrated voice response (IVR) operating system (OS) and associated software for each system within the architecture providing FTI to a customer; 3. mobile devices; 4. multi-functional devices (MFDs); 5. storage area network (SAN) components; 6. virtual desktop infrastructure (VDI) components such as the hypervisor and management console; 7. virtual machine (VM) and hypervisor/host OS software for each system within a virtual environment; 8. voice over IP (VoIP) systems; 9. each system within the architecture that receives, processes, stores or transmits FTI through a web-based system or website; and 10. each system within the agency's network that transmits FTI through a wireless local area network (WLAN). In particular, to use a virtual environment that receives, processes, stores or transmits FTI, the VMs and hypervisor/host operating system (OS) software for each system within the virtual environment that receives, processes, stores, or transmits FTI must be configured such that: 1. special VM functions available to system administrators in a virtualized environment that can leverage the shared memory space in a virtual environment, between the hypervisor and VM, are disabled; and 2. virtual systems are configured to prevent FTI from being dumped outside of the VM when system errors occur. The organization provides a detailed definition of configurations and the functions of the hardware and software involved in a data warehouse. To access FTI using a web browser, the agency must meet the following mandatory requirements: 1. private browsing must be enabled on the web browser and configured to delete temporary files and cookies upon exiting the session;

	2. Security enhancements, such as pop-up blocker and content filtering, must be enabled on the web browser; 3. Configure the designated web browser in accordance with the principle of least functionality and disable items, such as third-party add-ons.

Level HIX Implementation Requirements

Level HIX Implementation:	Security configuration guidelines may be developed by different federal agencies, so it is possible that a guideline could include configuration information that conflicts with another agency or the organization's guideline. HHS-specific, minimum-security configurations are used for the following Operating System (OS) and Applications: HHS FDCC Windows XP Standard, HHS FDCC Windows Vista Standard, Blackberry Server, and Websense; and, for all other OS's and applications, and to resolve configuration conflicts among multiple security guidelines, the organization uses the CMS hierarchy for implementing security configuration guidelines. If formal government-authored checklists do not exist, then organizations use vendor or industry group guidance, if available. The organization also ensures checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available). The organization analyzes changes to an information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice. Processing or storing of personally identifiable information (PII) in test environments is prohibited.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The organization requires the developer of the information system, system component, or information system service to (i) perform configuration management during system, component, or service development, implementation, and operation; (ii) document, manage, and control the integrity of changes to configuration items under configuration management; (iii) implement only organization-approved changes to the system, component, or service; (iv) document approved changes to the system, component, or service and the potential security impacts of such changes; and (v) track security flaws and flaw resolution within the system, component, or service, and report findings to defined personnel or roles (defined in the applicable system security plan).

Level PCI Implementation Requirements

Level PCI Implementation:	Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.

Control Reference: 10.l Outsourced Software Development

Control Specification:	Outsourced software development shall be supervised and monitored by the organization. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Documentation and Records; Media and Assets; Requirements (Legal and Contractual); Services and Acquisitions

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to Texas Health and Safety Code
Level 1 Implementation:	Where software development is outsourced, the following points are addressed contractually (either in a contract or Security Service Level Agreement): 1. licensing arrangements, code ownership, and intellectual property rights (see 6.b); 2. certification of the quality and accuracy of the work carried out; 3. escrow arrangements in the event of failure of the third-party; 4. rights of access for audit of the quality and accuracy of work done; 5. contractual requirements for quality and security functionality of code; and 6. testing before installation to detect malicious code.
Level 1 Control Standard Mapping:	CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 SA-11 (HIGH; MOD) CMSRs v3.1 SA-13 (HIGH) FedRAMP SA-11 FFIEC IS v2016 A.6.28(b) ISO/IEC 27001:2013 8.1 ISO/IEC 27002:2013 14.2.7 ISO/IEC 27799:2016 14.2.7 MARS-E v2 SA-11 NIST Cybersecurity Framework v1.1 DE.CM-4 NIST Cybersecurity Framework v1.1 ID.BE-1 NIST Cybersecurity Framework v1.1 ID.RA-3 NIST Cybersecurity Framework v1.1 ID.RA-6 NIST Cybersecurity Framework v1.1 PR.AT-3

Level 2 Implementation Requirements	
Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to FISMA Compliance Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The development of all outsourced software is supervised and monitored by the organization and must include security requirements, independent security review of the

	outsourced environment by a certified individual, certified security training for outsourced software developers, and code reviews. Certification for the purposes of this control is defined as a legally recognized license or certification in the legislative jurisdiction that the organization outsourcing the development has chosen as its domicile. The organization protects against supply chain threats by employing best practices and methodologies, such as including the security organization in all IT procurement considerations.
Level 2 Control Standard Mapping:	CSA CCM v3.0.1 CCC-02 FFIEC IS v2016 A.6.28 FFIEC IS v2016 A.6.28(b) FFIEC IS v2016 A.6.28(d) ISO/IEC 27002:2013 14.2.7 ISO/IEC 27799:2016 14.2.7 NIST Cybersecurity Framework v1.1 DE.CM-6 NIST Cybersecurity Framework v1.1 PR.AT-3

Level CMS Implementation Requirements

Level CMS Implementation:	The organization protects against supply chain threats by employing best practices and methodologies, wherever possible, selecting components that have been previously reviewed by other government entities (e.g., National Information Assurance Partnership [NIAP]) as part of a comprehensive, defense-in-breadth information security strategy.

Objective Name: 10.06 Technical Vulnerability Management

Control Objective:	To reduce the risks resulting from exploitation of published technical vulnerabilities, technical vulnerability management shall be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness.

Control Reference: 10.m Control of Technical Vulnerabilities

Control Specification:	Timely information about technical vulnerabilities of information systems being used shall be obtained; the organization's exposure to such vulnerabilities evaluated; and appropriate measures taken to address the associated risk. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Incident Response; IT Organization and Management Roles and Responsibilities; Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to State of Massachusetts Data Protection Act

Level 1 Implementation:	Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment (e.g., what software is installed on what systems) and the person(s) within the organization responsible for the software. Appropriate, timely action is taken in response to the identification of potential technical vulnerabilities. Once a potential technical vulnerability has been identified, the organization identifies the associated risks and the actions to be taken. Such action involves patching of vulnerable systems and/or applying other controls.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 201 CMR 17.04(6) CMSRs v3.1 RA-05 (HIGH; MOD) CRR v2016 VM:G2.Q1 CRR v2016 VM:G2.Q5 CRR v2016 VM:MIL2.Q4 CRR v2016 VM:MIL3.Q4 CSA CCM v3.0.1 TVM-02 FedRAMP RA-5 FFIEC IS v2016 A.4.4 FFIEC IS v2016 A.6.13 FFIEC IS v2016 A.8.3 IRS Pub 1075 v2016 9.3.5.6 ISO/IEC 27002:2013 12.6.1 ISO/IEC 27799:2016 12.6.1 MARS-E v2 RA-5 NIST Cybersecurity Framework v1.1 ID.RA-1 NIST Cybersecurity Framework v1.1 ID.RA-2 NIST Cybersecurity Framework v1.1 ID.RA-4 NIST Cybersecurity Framework v1.1 ID.RA-6 NIST Cybersecurity Framework v1.1 RS.MI-3 PMI DSP Framework PR.IP-2

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to CMMC Level 2 Subject to CMMC Level 5 Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Supplemental Requirements
Level 2 Implementation:	Level 1 plus:

The organization defines and establishes the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking, and any coordination responsibilities required.

Information resources (including tools and vulnerability mailing lists/other information sources), that will be used to identify relevant technical vulnerabilities and to maintain awareness about them, are identified for software and other technology (based on the asset inventory list, see 7.a). These information resources are updated based on changes in the inventory, or when other new or useful resources are found.

Internal and external vulnerability assessments of sensitive information systems (e.g., systems containing covered information, cardholder data) and networked environments are performed on a quarterly basis, and after any significant change in the network (e.g., new system component installations, changes in network topology, firewall rule modifications, product upgrades), by a qualified individual. These tests include both network- and application-layer tests.

Security vulnerability assessment tools or services accommodate the virtualization technologies used by the organization (e.g., virtualization aware).

The action taken is carried out according to the controls related to change management (see 10.k) or by following information security incident response procedures (see 11.c).

If a patch is available, change control procedures for the implementation of security patches and software modifications are followed (see 09.b). This includes assessing the risks associated with installing the patch (i.e., the risks posed by the vulnerability are compared with the risk of installing the patch). Patches are tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated.

If no patch is available, is delayed, or not applied, other controls are applied including:

1. documentation of impact;
2. documented change approval by authorized parties;
3. functionality testing to verify that the change does not adversely impact the security of the system;
4. back-out procedures;
5. turning off services or capabilities related to the vulnerability;
6. adapting or adding access controls (e.g., firewalls) at network borders (see 9.m);
7. increased monitoring to detect or prevent actual attacks; and
8. raising awareness of the vulnerability.

An audit log is kept for all procedures undertaken.

Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. The risk ranking considers the CVSS score, classification of the vendor supplied patch, and/or the classification and criticality of the affected system. The technical vulnerability management process is evaluated on a quarterly basis in order to ensure its effectiveness and efficiency. Systems at high risk are addressed first.

The configuration standards are required by CSF control 10.k for all system components (e.g., workstations, databases, servers, operating systems, applications, routers, switches, wireless access points). The standards are hardened to address, to the extent practical, all known security vulnerabilities. In particular, laptops, workstations, and servers are configured so they will not auto-run content from removable media (e.g., USB tokens, i.e., thumb drives; USB hard drives; CDs/DVDs; FireWire devices; external serial advanced technology attachment devices; and mounted network shares).

The organization's configuration standards are consistent with industry-accepted system hardening standards, including:

	1. Center for Internet Security (CIS); 2. International Organization for Standardization (ISO); 3. SysAdmin Audit Network Security (SANS); and 4. National Institute of Standards Technology (NIST); Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure (e.g., use secured technologies such as SSH, S-FTP, TLS 1.2 or later, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.). The organization conducts both internal and external penetration testing, within every 365 days, on defined information systems or system components. A prioritization process is implemented to determine which patches are applied across the organizations systems. Patches installed in the production environment are also installed in the organizations disaster recovery environment in a timely manner.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC7.1 AICPA 2017 CC7.4 CIS CSC v7.1 18.11 CIS CSC v7.1 3.7 CIS CSC v7.1 5.1 CMMC v1.0 RM.2.143-0 CMMC v1.0 SC.5.230-0 CMSRs v3.1 CM-06 (HIGH; MOD) CMSRs v3.1 CM-07 (HIGH; MOD) CMSRs v3.1 RA-05 (HIGH) CMSRs v3.1 RA-05 (HIGH; MOD) CRR v2016 CCM:G2.Q7 CRR v2016 VM:G1.Q1 CRR v2016 VM:G1.Q5 CRR v2016 VM:G2.Q4 CRR v2016 VM:G2.Q5 CRR v2016 VM:G3.Q2 CRR v2016 VM:G3.Q3 CRR v2016 VM:G4.Q1 CRR v2016 VM:MIL2.Q2 CRR v2016 VM:MIL2.Q4 CRR v2016 VM:MIL3.Q2 CRR v2016 VM:MIL3.Q4 CRR v2016 VM:MIL4.Q1 CRR v2016 VM:MIL4.Q2 CSA CCM v3.0.1 IVS-05 FedRAMP CM-6 FedRAMP RA-5 FFIEC IS v2016 A.10.1 FFIEC IS v2016 A.10.3(c) FFIEC IS v2016 A.6.13 FFIEC IS v2016 A.6.15(c) FFIEC IS v2016 A.6.15(d) FFIEC IS v2016 A.6.15(f) FFIEC IS v2016 A.6.15(h) FFIEC IS v2016 A.6.27(d) FFIEC IS v2016 A.8.1(c) FFIEC IS v2016 A.8.3 FFIEC IS v2016 A.8.4 IRS Pub 1075 v2016 9.3.14.3 IRS Pub 1075 v2016 9.3.5.6 IRS Pub 1075 v2016 9.3.5.7 ISO/IEC 27002:2013 12.6.1 ISO/IEC 27799:2016 12.6.1 MARS-E v2 CM-6 MARS-E v2 CM-7 MARS-E v2 RA-5 NIST 800-171 r2 3.11.3-0 NIST Cybersecurity Framework v1.1 DE.CM-8

	NIST Cybersecurity Framework v1.1 DE.DP-5 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 ID.RA-1 NIST Cybersecurity Framework v1.1 ID.RA-2 NIST Cybersecurity Framework v1.1 ID.RA-5 NIST Cybersecurity Framework v1.1 PR.IP-12 NIST Cybersecurity Framework v1.1 RS.CO-3 NIST Cybersecurity Framework v1.1 RS.MI-3 NIST SP 800-53 R4 CM-7a[HML]{1} NIST SP 800-53 R4 CM-7b[HML]{2} NIST SP 800-53 R4 SA-15(7)b[S]{0} NIST SP 800-53 R4 SA-15(7)c[S]{0} NIST SP 800-53 R4 SC-7(17)[S]{0} NY DOH SSP v3.1 CM-7a[M]-0 NY DOH SSP v3.1 CM-7b[M]-1 NY DOH SSP v3.1 SI-2.IS1a[HML]-0 NY DOH SSP v3.1 SI-2b[M]-0 PCI DSS v3.2.1 11.2 PCI DSS v3.2.1 11.2.1 PCI DSS v3.2.1 11.2.2 PCI DSS v3.2.1 11.2.3 PCI DSS v3.2.1 2.2 PCI DSS v3.2.1 2.2.2 PCI DSS v3.2.1 2.2.3 PCI DSS v3.2.1 6.1 PCI DSS v3.2.1 6.4.5 PMI DSP Framework PR.IP-2 SR v6.4 2-0 SR v6.4 32-2 SR v6.4 32b-0

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to 23 NYCRR 500 Subject to Banking Requirements Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 2 Subject to CMMC Level 4 Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)

Level 3 Implementation:	Level 2 plus: Perform an enterprise security posture review annually. The organization employs automated mechanisms monthly to determine the state of information system components with regard to flaw remediation. Vulnerability scanning tools are updated regularly with all relevant information system vulnerabilities. The organization scans for vulnerabilities in the information system and hosted applications within every 30 days and when new vulnerabilities potentially affecting the systems and networked environments are identified and reported. The organization updates the list of information system vulnerabilities scanned at least weekly and when new vulnerabilities potentially affecting the systems and networked environments are identified and reported. The organization includes privileged access authorization to operating system, telecommunications, and configuration components for selected vulnerability scanning activities, to facilitate more thorough scanning. The organization conducts regular penetration testing, no less than every 365 days on defined information systems or system components, to identify vulnerabilities and attack vectors that can be used to successfully exploit enterprise systems. Penetration testing occurs from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization), as well as from within its boundaries (i.e., on the internal network), to simulate both outsider and insider attacks. This includes tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, emails or documents containing passwords or other information critical to system operation. The organization conducts regular penetration testing, no less than every 365 days, on defined information systems or system components to identify vulnerabilities and attack vectors that can be used to successfully exploit enterprise systems. Penetration testing occurs from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks. This includes tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, emails or documents containing passwords or other information critical to system operation. The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components. The organization employs vulnerability scanning procedures that can identify the breadth and depth of coverage (i.e., information system components scanned, and vulnerabilities checked). The organization reviews historic audit logs to determine high vulnerability scan findings identified in the information system has been previously exploited.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMMC v1.0 CA.4.164-1 CMMC v1.0 CA.4.164-2 CMMC v1.0 CA.4.227-0 CMMC v1.0 RM.2.142-0 CMSRs v3.1 CA-02 (HIGH; MOD) CMSRs v3.1 CA-08 (HIGH; MOD) CMSRs v3.1 RA-05 (HIGH; MOD) CMSRs v3.1 RA-05(01) (HIGH; MOD) CMSRs v3.1 RA-05(02) (HIGH; MOD) CMSRs v3.1 RA-05(04) (HIGH)

	CMSRs v3.1 SI-02 (HIGH; MOD) CMSRs v3.1 SI-02(01) (HIGH) CMSRs v3.1 SI-02(02) (HIGH; MOD) COBIT 5 DS5.9 COBIT 5 DSS05.02 CRR v2016 VM:G2.Q2 CRR v2016 VM:G2.Q3 CSA CCM v3.0.1 TVM-02 FedRAMP CA-8 FedRAMP CA-8(1) FedRAMP RA-5 FedRAMP RA-5(1) FedRAMP RA-5(3) FedRAMP RA-5(5) FedRAMP RA-5(8) FedRAMP SI-2 FedRAMP SI-2(2) FFIEC IS v2016 A.8.1(d) IRS Pub 1075 v2016 9.3.14.3 IRS Pub 1075 v2016 9.3.17.2 IRS Pub 1075 v2016 9.4.14 IRS Pub 1075 v2016 9.4.15 IRS Pub 1075 v2016 9.4.16 IRS Pub 1075 v2016 9.4.17 MARS-E v2 CA-2 MARS-E v2 PE-2(2) MARS-E v2 RA-5 MARS-E v2 RA-5(1) MARS-E v2 SI-2 MARS-E v2 SI-2(1) MARS-E v2 SI-2(2) NIST 800-171 r2 3.11.2-0 NIST Cybersecurity Framework v1.1 DE.CM-8 NIST Cybersecurity Framework v1.1 ID.RA-1 NIST Cybersecurity Framework v1.1 PR.PT-3 NIST Cybersecurity Framework v1.1 RS.MI-3 NIST SP 800-53 R4 AC-4(11)[S]{0} NIST SP 800-53 R4 CA-8(1)[S]{0} NIST SP 800-53 R4 CA-8(2)[S]{0} NIST SP 800-53 R4 CA-8[H]{0} NIST SP 800-53 R4 RA-5(1)[HM]{0} NIST SP 800-53 R4 RA-5(2)[HM]{0} NIST SP 800-53 R4 RA-5(3)[S]{0} NIST SP 800-53 R4 RA-5(5)[HM]{0} NIST SP 800-53 R4 RA-5(8)[S]{0} NIST SP 800-53 R4 RA-5a[HML]{0} NIST SP 800-53 R4 SA-12(11)[S]{0} NIST SP 800-53 R4 SA-15(7)a[S]{0} NIST SP 800-53 R4 SI-2(2)[HM]{0} NRS 603A.215.1 NY DOH SSP v3.1 AC-5.IS5[M]-0 NY DOH SSP v3.1 CA-8.NYSc[MN]-0 NY DOH SSP v3.1 RA-5(1)[M]-0 NY DOH SSP v3.1 RA-5(3).IS1[M]-0 NY DOH SSP v3.1 RA-5(3).IS2[M]-0 NY DOH SSP v3.1 RA-5(3)[M]-0 NY DOH SSP v3.1 RA-5.IS1[HML]-0 PCI DSS v3.2.1 11.3 PCI DSS v3.2.1 11.3.1 PCI DSS v3.2.1 11.3.2 PCI DSS v3.2.1 11.3.3 PCI DSS v3.2.1 11.3.4 PCI DSS v3.2.1 6.2

Level CIS Implementation Requirements

Level CIS Implementation:	Organizations install the latest stable version of any security-related updates on all network devices.

	The organization deploys automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor. The organization performs periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively. The organization establishes a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks. The organization uses vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments are used as a starting point to guide and focus penetration testing efforts. The organization ensures, wherever possible, that Red Team results are documented using open, machine-readable standards (e.g., SCAP) and devises a scoring method for determining the results of Red Team exercises, so that results can be compared over time. Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems. The organization uses a dedicated account, which is tied to specific machines at specific IP addresses and not used for any other administrative activities, is used for authenticated vulnerability scans. The organization utilizes an up-to-date Security Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems. The organization uses automated patch management tools and software update tools for the operation system and/or software/applications on all information systems for which such tools are available and determined to be safe. The organization regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner. The organization documents security configuration standards for all authorized operating systems and software.

Level CMS Implementation Requirements

Level CMS Implementation:	The organization corrects identified information system flaws on production equipment within 10 business days and all others within 30 calendar days. A risk-based decision is documented through the configuration management process in the form of written authorization from the CMS CIO, or his/her designated representative (e.g., the system data owner or CMS CISO), if a security patch is not applied to a security-based system or network. For critical infrastructure and systems (e.g., public-facing, Internet accessible), critical security patches are applied within one month of release. For less-critical infrastructure and systems (e.g., only accessible internally) or for non-critical security patches, patches are applied within three months of release.

	The organization attempts to determine what information about the information system environment is discernible by adversaries and subsequently takes appropriate corrective action to limit discoverable system information. The organization centrally manages the flaw remediation process and installs software updates, automatically where possible. The organization conducts both internal and external penetration testing, within every 365 days, on defined information systems or system components (defined in the applicable system security plan), or whenever there has been a significant change to the system. As a minimum, penetration testing must be conducted to determine: 1. how well the system tolerates real world-style attack patterns; 2. the likely level of sophistication an attacker needs to successfully compromise the system; 3. additional countermeasures that could mitigate threats against the system; and, 4. defenders' ability to detect attacks and respond appropriately. Penetration testing is required under OMB M-17-09 for all systems defined as High Value Assets (HVAs).

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The organization mitigates legitimate high-risk vulnerabilities within 30 days and moderate risk vulnerabilities within 90 days. The organization updates the list of information system vulnerabilities scanned prior to a new scan or when new vulnerabilities are identified and reported. The organization includes privileged access authorization to operating systems, web applications, databases, telecommunications, and configuration components for selected vulnerability scanning activities to facilitate more thorough scanning. The organization requires the developer of the information system, system component, or information system service to employ static and dynamic code analysis tools to identify common flaws and document the results of the analysis. The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service. The organization installs security-relevant software and firmware updates within 30 days of release of the updates and incorporates flaw remediation into the organizational configuration management process. The organization measures the time between flaw identification and flaw remediation and further a specific time-period based on the criticality of the flaw for taking corrective actions. The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

Level FFIEC IS Implementation Requirements

Level FFIEC IS Implementation:	The organization conducts both internal and external penetration testing as needed but no less than once within every 365 days, in accordance with the organizations information security procedures and results are reported to management.

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation:	At a minimum, systems containing FTI are scanned quarterly to identify any vulnerability in the information system. Multifunction Device (MFD) firmware is supported by the vendor and is kept up to date with the most current firmware available. Vulnerability assessments must be performed on systems in a virtualized environment prior to system implementation and frequently thereafter. To use a VoIP network that provides FTI to a customer, each system within the agency's network that transmits FTI to an external customer through the VoIP network is subject to frequent vulnerability testing. To use an external web-based system or website that provides FTI over the Internet to a customer, the agency must ensure each system within the architecture that receives, processes, stores, or transmits FTI to an external customer through the web-based system or website is subject to frequent vulnerability testing. To access FTI using a web browser, the agency must install vendor-specified security patches and hot fixes regularly for the web browser, add-ons, and Java. To use FTI in an 802.11 WLAN, the agency must conduct vulnerability scanning as part of periodic technical security assessments for the organization's WLAN.

Level HIX Implementation Requirements	
Level HIX Implementation:	Perform external network penetration testing and conduct an enterprise security posture review as needed but no less than once within every 365 days, in accordance with organizational information security procedures. The organization mitigates legitimate high-risk vulnerabilities within 30 days and moderate risk vulnerabilities within 90 days. The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis as part of its authorization package (see also 09.i) and updates the report in any reauthorization action. The organization installs security-relevant software and firmware updates on production equipment within a timeframe based on the National Vulnerability Database (NVD) Vulnerability Severity Rating of the flaw as follows: High severity within 7 calendar days, medium severity within 15 calendar days, and all others within 30 calendar days. The organization incorporates flaw remediation into the organizational configuration management process, with risk-based decisions if a security patch is not applied to a security-based system or network authorized by the organization.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation:	The organization identifies vulnerabilities exploited during a security incident and implements security safeguards to reduce risk and vulnerability exploit exposure, including isolating or disconnecting systems. All systems must be scanned for vulnerabilities before being installed in production and periodically thereafter.

	Where a SE has outsourced a system to another SE or a third party, vulnerability scanning/penetration testing must be coordinated. Scanning/testing and mitigation must be included in third party agreements. The output of the scans/penetration tests will be reviewed in a timely manner by the system owner. Copies of the scan report/penetration test must be shared with the ISO/designated security representative for evaluation of risk. The organization scans for vulnerabilities in the information system and hosted applications no less often than once every seventy-two [72] hours and when new vulnerabilities potentially affecting the system/applications are identified and reported. The organization employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: (i) enumerating platforms, software flaws, and improper configurations; (ii) formatting checklists and test procedures; (iii) measuring vulnerability impact; (iv) complying with DHS Continuous Diagnostics and Mitigation program and CMS requirements; and (v) complying with required reporting metrics (e.g., CyberScope). The organization employs automated mechanisms no less often than once every seventy-two [72] hours to determine the state of information system components regarding flaw remediation.

Level PCI Implementation Requirements

Level PCI Implementation:	Perform quarterly internal vulnerability scans and rescans, which may be automated, manual, or a combination thereof, as needed, until all 'high-risk' vulnerabilities are resolved in accordance with the organization's vulnerability rankings. Scans must be performed by qualified personnel. Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel. Implement a methodology for penetration testing that: 1. is based on industry-accepted penetration testing approaches (e.g., NIST SP 800-115); 2. includes coverage for the entire card data environment (CDE) perimeter and critical systems; 3. includes testing from both inside and outside the network; 4. includes testing to validate any segmentation and scope-reduction controls; 5. defines application-layer penetration tests to include, at a minimum, the vulnerabilities identified in 10.b, level 1 (reference PCI DSS v3 6.5); 6. defines network-layer penetration tests to include components that support network functions as well as operating systems; 7. includes review and consideration of threats and vulnerabilities experienced in the last 12 months; and 8. specifies retention of penetration testing results and remediation activities results. If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in the CDE. For organizations assessed as a service provider, penetration

	testing on segmentation controls are performed at least every six months and after any changes to segmentation controls/methods.

Level Supplemental Requirements	Implementation Requirements
Level Supplemental Requirements Implementation:	Maintain and adhere to a documented process to remediate all critical, high, and medium risk security vulnerabilities promptly.

Control Category: 11.0 - Information Security Incident Management

Objective Name: 11.01 Reporting Information Security Incidents and Weaknesses

Control Objective:	To ensure information security events and weaknesses associated with information systems are handled in a manner allowing timely corrective action to be taken.

Control Reference: 11.a Reporting Information Security Events

Control Specification:	Information security events shall be reported through appropriate communications channels as quickly as possible. All employees, contractors and third-party users shall be made aware of their responsibility to report any information security events as quickly as possible. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Awareness and Training; Incident Response; IT Organization and Management Roles and Responsibilities; Personnel; Policies and Procedures; Risk Management and Assessments; Third-parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 3 Subject to NIST 800-171 Basic Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to SCIDSA Requirements Subject to State of Massachusetts Data Protection Act Subject to Supplemental Requirements Subject to Texas Health and Safety Code
Level 1 Implementation:	Formal information security event reporting procedures to support the corporate direction (policy) are established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security event, treating the breach as discovered, and the timeliness of reporting and response. Organization-wide standards are specified for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that is included in the incident notification. This reporting also includes notifying internal and external stakeholders, the appropriate Community Emergency Response Team, and law enforcement agencies in accordance with all legal or regulatory requirements for involving that organization in computer incidents. With the importance of Information Security Incident Handling, a policy is established to set the direction of management.

	A point of contact is established for the reporting of information security events. It is to be ensured that this point of contact is known throughout the organization, is always available, and is able to provide adequate and timely response. The organization also maintains a list of third-party contact information (e.g., the email addresses of their information security officers), which can be used to report a security incident. Employees and other workforce members, including third-parties, are able to freely report security weaknesses (real and perceived) without fear of repercussion. The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team. Organizations ensure workforce members do not interfere with federal or state investigations or disciplinary proceedings by willful misrepresentation or omission of facts or by the use of threats or harassment against any person. Organizations ensure violations of these requirements are incorporated into disciplinary procedures (see 02.f).
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(2) 1 TAC § 390.2(a)(4)(A)(ix) 1 TAC § 390.2(a)(4)(A)(xi) 1 TAC § 390.2(a)(4)(B)(xvi) 1 TAC § 390.2(a)(4)(B)(xviii)(III) 1 TAC § 390.2(a)(4)(B)(xviii)(IV) 201 CMR 17.03(2)(j) AICPA 2017 CC7.3 AICPA 2017 CC7.4 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CIS CSC v7.1 19.4 CIS CSC v7.1 19.5 CMMC v1.0 IR.3.098-1 CMSRs v3.1 IR-01 (HIGH; MOD) CMSRs v3.1 PM-12 (HIGH; MOD) CRR v2016 IM:G1.Q1 CRR v2016 IM:G3.Q1 CRR v2016 IM:G3.Q2 CRR v2016 IM:G4.Q2 CRR v2016 IM:MIL2.Q2 CSA CCM v3.0.1 SEF-03 FedRAMP IR-1 FFIEC IS v2016 A.6.21(b) FFIEC IS v2016 A.8.1(j) FFIEC IS v2016 A.8.5(a) FFIEC IS v2016 A.8.5(d) FFIEC IS v2016 A.8.5(e) FFIEC IS v2016 A.8.5(f) FFIEC IS v2016 A.8.5(g) IRS Pub 1075 v2016 9.3.8.1 ISO/IEC 27002:2013 16.1.1 ISO/IEC 27002:2013 16.1.2 ISO/IEC 27002:2013 16.1.3 ISO/IEC 27799:2016 16.1.1 ISO/IEC 27799:2016 16.1.2 ISO/IEC 27799:2016 16.1.3 MARS-E v2 IR-1 MARS-E v2 PM-12 NIST 800-171 r2 3.6.2-1 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST Cybersecurity Framework v1.1 PR.IP-9 NIST Cybersecurity Framework v1.1 RS.CO-2 NIST Cybersecurity Framework v1.1 RS.CO-3 NIST Cybersecurity Framework v1.1 RS.CO-5 NIST SP 800-53 R4 IR-4(6)[S]{0} NIST SP 800-53 R4 IR-4(7)[S]{0} NIST SP 800-53 R4 IR-4(9)[S]{0} NIST SP 800-53 R4 PM-12[HML]{0} NIST SP 800-53 R4 SI-4(19)[S]{1} NY DOH SSP v3.1 IR-1[M]-1 NY DOH SSP v3.1 IR-5.IS1a[HML]-0 NY DOH SSP v3.1 IR-5.IS1b[HML]-0

	NY DOH SSP v3.1 IR-6.IS.CSP1[HML]-2 NY DOH SSP v3.1 IR-6b[M]-0 NY DOH SSP v3.1 PM-12[M]-0 NY DOH SSP v3.1 PM-16[M]-2 PCI DSS v3.2.1 12.10 PCI DSS v3.2.1 12.10.3 PMI DSP Framework DE-4 PMI DSP Framework RS-1 SCIDSA 33-99-20(H) SR v6.4 34b.i-0 SR v6.4 34b.ii-0 SR v6.4 35-0

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to 23 NYCRR 500 Subject to Banking Requirements Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 4 Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to HIPAA Breach Notification Subject to HITRUST De-ID Framework Requirements Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to SCIDSA Requirements Subject to the CMS Minimum Security Requirements (High) Subject to the State of Nevada Security of Personal Information Requirements
Level 2 Implementation:	Level 1 plus: The policy refers to the specific procedures and programs to address incidents and also refers to a forensic program. The organization institutes a mechanism to anonymously report security issues. Procedures are developed to provide for the definition and assessment of information security incidents (e.g., an event/incident classification scale to decide whether an event classifies as an incident), roles and responsibilities, incident handling, and reporting and communication processes. The organization formally assigns job titles and duties for handling computer and network security incidents to specific individuals and identifies management personnel who will support the incident handling process by acting in key decision-making roles. The procedures also state the requirements for an incident handling team to address regulatory requirements, third-

party relationships, and the handling of third-party security breaches. Reports and communications are made without unreasonable delay and no later than 60 days after the discovery of the incident, unless otherwise stated by law enforcement in writing or orally. If the statement is made in writing, the notification is delayed for the time specified by the official. If the statement is made orally, the organization documents the statement, including the identity of the official making the statement, and delays the notification temporarily and no longer than 30 days from the date of the oral statement, unless a written statement from a law enforcement official is submitted during that time.

All employees, contractors and third-party users receive mandatory incident response training to ensure they are aware of their responsibilities to report any information security events as quickly as possible, the procedure for reporting information security events and the point(s) of contact, including the incident response team, and the contact information is published and made readily available.

The reporting procedures include:

1. feedback processes to ensure that those reporting information security events are notified of results after the issue has been dealt with and closed;
2. information security event reporting forms to support the reporting action, and to help the person reporting to remember all necessary actions in case of an information security event including:
    i. the correct behavior to be undertaken in case of an information security event and immediately noting all important details (e.g., type of non-compliance or breach) occurring malfunction, messages on the screen, strange behavior; and
    ii. not carrying out any own action, but immediately reporting to the point of contact;
3. reference to an established formal disciplinary process for dealing with employees, contractors or third-party users who commit security breaches;
4. communication with each individual affected by, or who is reasonably believed to have been affected by, the incident;
5. communication with business associate(s) identifying each individual affected by, or who is reasonably believed to have been affected by, the incident;
6. communicating incidents to local and federal law enforcement agencies; and
7. automated workflow processes for incident management, reporting and resolution.

Reports to the individuals affected by the incident are provided with notification by first-class mail to the individual (or the next of kin of the individual if the individual is deceased) at the last known address of the individual or the next of kin, respectively, or by electronic mail if specified as a preference by the individual. Organizations may provide notifications by telephone in cases deemed urgent by the organization. In the case that there are 10 or more individuals for whom there is insufficient or out-of-date contact information (including a phone number, email address, or any other form of appropriate communication), a conspicuous posting is placed on the home page of the website of the organization involved for a period of 90 days. A toll-free phone number that remains active for at least 90 days is also posted where an individual can learn whether the individual's information may be included in the breach. For fewer than 10 individuals, a substitute form of notice reasonably calculated to reach the individual is provided, except when there is insufficient or out-of-date information that precludes written notification to the next of kin or personal representative. The organization also notifies, without unreasonable delay, any consumer reporting agency of the time the notification is distributed and the content of the notification.

If more than 500 residents of such State or jurisdiction were, or are reasonably believed to have been, affected by the breach, notice is immediately provided to the federal government (to publicly disclose) and prominent media outlets.

	The notification to individuals is written in plain language (e.g., at an appropriate reading level, using clear language and syntax, and does not include any extraneous material that might diminish the message it is trying to convey). Alerts from the organization's intrusion detection and intrusion prevention systems are utilized for reporting information security events.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.404(b) HIPAA.BN-0 45 CFR Part § 164.404(c)(1)(A) HIPAA.BN-0 45 CFR Part § 164.404(c)(1)(B) HIPAA.BN-0 45 CFR Part § 164.404(c)(1)(C) HIPAA.BN-0 45 CFR Part § 164.404(c)(1)(D) HIPAA.BN-0 45 CFR Part § 164.404(c)(1)(E) HIPAA.BN-0 45 CFR Part § 164.406(b) HIPAA.BN-0 45 CFR Part § 164.406(c) HIPAA.BN-0 45 CFR Part § 164.410(a)(1) HIPAA.BN-2 45 CFR Part § 164.410(b) HIPAA.BN-0 45 CFR Part § 164.412(a) HIPAA.BN-0 45 CFR Part § 164.412(b) HIPAA.BN-0 AICPA 2017 CC2.2 AICPA 2017 CC2.3 AICPA 2017 CC7.3 AICPA 2017 CC7.4 AICPA 2017 CC7.5 AICPA 2017 P6.5 CIS CSC v7.1 19.1 CIS CSC v7.1 19.2 CIS CSC v7.1 19.3 CIS CSC v7.1 19.6 CMMC v1.0 AT.4.059-1 CMSRs v3.1 IR-01 (HIGH; MOD) CMSRs v3.1 IR-02 (HIGH) CMSRs v3.1 IR-02 (HIGH; MOD) CMSRs v3.1 IR-04 (HIGH; MOD) CMSRs v3.1 IR-06 (HIGH; MOD) CMSRs v3.1 IR-06(01) (HIGH; MOD) CMSRs v3.1 PM-12 (HIGH; MOD) COBIT 5 DS5.6 COBIT 5 DSS02.01 COBIT 5 DSS05.07 CRR v2016 IM:G1.Q3 CRR v2016 IM:G1.Q4 CRR v2016 IM:G2.Q1 CRR v2016 IM:G3.Q2 CRR v2016 IM:G4.Q1 CRR v2016 IM:G4.Q2 CRR v2016 IM:G4.Q4 CRR v2016 IM:MIL2.Q1 CRR v2016 IM:MIL2.Q3 CRR v2016 IM:MIL3.Q1 CRR v2016 IM:MIL3.Q2 CRR v2016 IM:MIL4.Q1 CRR v2016 IM:MIL4.Q3 CRR v2016 IM:MIL5.Q1 CSA CCM v3.0.1 SEF-02 CSA CCM v3.0.1 SEF-03 CSA CCM v3.0.1 SEF-04 FedRAMP IR-1 FedRAMP IR-4 FedRAMP IR-6 FedRAMP IR-6(1) FFIEC IS v2016 A.6.21(b) FFIEC IS v2016 A.6.31(f) FFIEC IS v2016 A.8.1(b) FFIEC IS v2016 A.8.1(j) FFIEC IS v2016 A.8.5(a) FFIEC IS v2016 A.8.5(b) FFIEC IS v2016 A.8.5(d) FFIEC IS v2016 A.8.5(e) FFIEC IS v2016 A.8.5(f) FFIEC IS v2016 A.8.5(g) IRS Pub 1075 v2016 9.3.8.1

	IRS Pub 1075 v2016 9.3.8.2 IRS Pub 1075 v2016 9.3.8.6 ISO/IEC 27002:2013 16.1.1 ISO/IEC 27002:2013 16.1.4 ISO/IEC 27002:2013 7.2.1 ISO/IEC 27002:2013 7.2.2 ISO/IEC 27799:2016 16.1.1 ISO/IEC 27799:2016 16.1.4 ISO/IEC 27799:2016 7.2.1 ISO/IEC 27799:2016 7.2.2 MARS-E v2 IR-1 MARS-E v2 IR-2 MARS-E v2 IR-4(1) MARS-E v2 IR-6 MARS-E v2 IR-6(1) MARS-E v2 PM-12 NIST Cybersecurity Framework v1.1 DE.CM-1 NIST Cybersecurity Framework v1.1 PR.AT-5 NIST Cybersecurity Framework v1.1 PR.IP-9 NIST Cybersecurity Framework v1.1 RS.CO-2 NIST SP 800-53 R4 AT-2(1)[S]{1} NIST SP 800-53 R4 IR-6(3)[S]{0} NIST SP 800-53 R4 IR-6a[HML]{0} NIST SP 800-53 R4 IR-7(2)b[S]{0} NIST SP 800-53 R4 IR-8a[HML]{2} NIST SP 800-53 R4 IR-8a[HML]{5} NIST SP 800-53 R4 SA-15(10)[S]{1} NIST SP 800-53 R4 SI-4a[HML]{0} NRS 603A.215.1 NY DOH SSP v3.1 SC-7.IS4b[M]-2 PCI DSS v3.2.1 12.10 PCI DSS v3.2.1 12.10.1 PCI DSS v3.2.1 12.10.4 PCI DSS v3.2.1 12.10.5 PMI DSP Framework DE-4 PMI DSP Framework RC-3 SCIDSA 33-99-20(H)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	
Level 3 Implementation:	Level 2 plus: A duress alarm is provided whereby a person under duress can indicate such problems. The procedures for responding to duress alarms reflect the high-risk situation such alarms are indicating. An information security assessment is made, either on all incidents or on a sample, to further validate the effectiveness or otherwise of established controls and of the risk assessment that led to them.

	Examples include: 1. a break-in leading to theft of IT hardware, resulting in a confidentiality breach; or 2. a fire could be set to disguise misuse of IT equipment.
Level 3 Control Standard Mapping:	ISO/IEC 27002:2013 16.1.2 ISO/IEC 27002:2013 16.1.6 ISO/IEC 27799:2016 16.1.2 ISO/IEC 27799:2016 16.1.6 NIST Cybersecurity Framework v1.1 DE.DP-4 NIST Cybersecurity Framework v1.1 PR.IP-7 NIST Cybersecurity Framework v1.1 PR.IP-9 NIST Cybersecurity Framework v1.1 RS.CO-2 NIST Cybersecurity Framework v1.1 RS.RP-1

Level CCPA	**Implementation Requirements**
Level CCPA Implementation:	Businesses are required to notify consumers if there is unauthorized access to the consumer's non-encrypted or non-redacted personal information due to the business's lack of sufficient security controls.

Level Cloud Service Providers	**Implementation Requirements**
Level Cloud Service Providers Implementation:	Cloud service providers make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).

Level CMS	**Implementation Requirements**
Level CMS Implementation:	The organization requires personnel to report actual or suspected security incidents to the organizational incident response capability within the timeframe established in the current CMS Incident Handling and Breach Notification Standard.

Level De-ID Data Environment	**Implementation Requirements**
Level De-ID Data Environment Implementation:	Entities receiving de-identified data notify the providing organization's data custodian of breaches involving Patient De-identified data as required by law for breaches of Patient Identifiable data, so that the providing organization can determine the appropriate response. Visitor-related incidents are tracked, and corrective actions are taken, when they occur.

Level FTI Custodians	**Implementation Requirements**
Level FTI Custodians Implementation:	Any data incident potentially involving FTI must immediately be reported to the appropriate Treasury Inspector General for Tax Administration (TIGTA) field office and the IRS Office of Safeguards immediately, but no later than 24 hours after identification of a possible issue involving FTI. To notify the Office of Safeguards, the agency must document the specifics of the incident known at that time into a data incident report including, but not limited to: 1. Name of agency and agency Point of Contact for resolving a data incident with contact information; 2. Date and time of the incident; 3. Date and time the incident was discovered; 4. How the incident was discovered;

	5. Description of the incident and the data involved, including specific data; 6. elements, if known; 7. Potential number of FTI records involved; if unknown, provide a range if possible; 8. Address where the incident occurred; 9. IT involved (e.g., laptop, server, mainframe); 10. Do not include any FTI in the data Incident report; and 11. Reports must be sent electronically and encrypted via IRS-approved encryption techniques. Use the term data incident report in the subject line of the email. The agency must inform the Office of Safeguards of notification activities undertaken before release to individuals impacted by a breach of FTI. In addition, the agency must inform the Office of Safeguards of any pending media releases, including sharing the text, prior to distribution.

Level GDPR Implementation Requirements	
Level GDPR Implementation:	In the case of a personal data breach, the controller notifies the appropriate supervisory authority, without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and liberties (freedoms) of natural persons; and such notification is provided all at once or, if in phases, without further undue delay; and contain at least: 1. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned; 2. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; 3. describe the likely consequences of the personal data breach; and 4. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. Where the notification to the supervisory authority is not made within 72 hours, it is accompanied by reasons for the delay. The processor notifies the controller without undue delay after becoming aware of a personal data breach. The controller documents any personal data breach, comprising the facts relating to the breach, its effects and the remedial action taken. With limited exception, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller communicates the personal data breach to the data subject without undue delay. Exceptions to notification occur when ANY of the following conditions are met: 1. the controller has implemented appropriate technical and organizational protection measures, and that those measures were applied to the personal data affected by the personal data breach, particularly those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption; 2. the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize; or 3. it would involve disproportionate effort. In such a case, there is instead a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

	The communication to the data subject describes in clear and plain language the nature of the personal data breach and contain at least: 1. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; 2. describe the likely consequences of the personal data breach; 3. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

Level HIPAA Implementation Requirements

Level HIPAA Implementation:	Reports to external organizations, individuals or federal or state agencies include: 1. a brief description of what happened; 2. the date of the breach; 3. the date of the discovery of the breach; 4. a description of the types of information that were involved in the breach (e.g., full name, Social Security number, date of birth, home address, account number, disability code); 5. the recommended steps external entities take to protect themselves from potential harm resulting from the breach; 6. a brief description of the steps the organization is taking to: i. investigate the breach, ii. mitigate damages, and iii. protect against any further breaches; and 7. contact procedures to ask questions or learn additional information, which include: i. a toll-free telephone number, ii. an email address, iii. website, or iv. postal address. Notifications to individuals affected by security events are written in plain language.

Level HIX Implementation Requirements

Level HIX Implementation:	The organization follows CMS Incident Reporting requirements for reporting incidents to oversight organizations.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The organization employs automated mechanisms to assist in the reporting of security incidents. The organization employs automated mechanisms to increase the availability of incident response-related information and support. The organization: (i) develops an incident response plan that: (a) provides the organization with a roadmap for implementing its incident response capability; (b) describes the structure and organization of the incident response capability; (c) provides a high-level approach for how the incident response capability fits into the overall organization; (d) meets the unique requirements of the organization, which relate to mission, size, structure, and functions; (e) defines reportable incidents; (f) provides metrics for measuring the incident response capability within the organization; (g) defines the resources and management support needed to effectively maintain and

	mature an incident response capability; and (h) is reviewed and approved by the applicable Incident Response Team Leader; (ii) distributes copies of the incident response plan to: (a) CMS Chief Information Security Officer; (b) CMS Chief Information Officer; (c) Information System Security Officer; (d) CMS Office of the Inspector General/Computer Crimes Unit; (e) all personnel within the organization Incident Response Team; (f) all personnel within the PII Breach Response Team; and (g) all personnel within the organization Operations Centers; (iii) reviews the incident response plan within every 365 days; (iv) updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; (v) communicates incident response plan changes to the organizational elements listed in (ii) above; and (vi) protects the incident response plan from unauthorized disclosure and modification. The organization reports findings to defined personnel or roles (defined in the applicable system security plan). Systems processing, storing, or transmitting PII (to include PHI): When defining the requirements for and designing an organization's insider threat program, the insider threat team must engage the participation, and obtain concurrence, of the organization's Privacy Officer prior to implementation; for existing insider threat programs, conduct a review of the program with the organization's Privacy Officer to ensure program meets applicable privacy requirements. The organization reports findings to defined personnel or roles (defined in the applicable system security plan).

Level PCI Implementation Requirements

Level PCI Implementation:	The organization designates specific personnel to be available on a 24/7 basis to respond to alerts.

Level SCIDSA Implementation Requirements

Level SCIDSA Implementation:	The licensee is required to report, at least annually, the overall status and compliance of the information security program, and any matters relevant to the program (e.g., risk assessments, events, violations, etc.). The licensee is required to notify the director no later than 72 hours after notification of a cybersecurity event if: 1. South Carolina is the licensee's state of domicile, or the licensee's home state in the case of a producer; or 2. The Licensee has reason to believe the information involved in the event involves no less than 250 consumers residing in the State and there's reasonable likelihood of harm to consumer residing in the State. The licensee provides, in electronic form, as much information as possible regarding the event, including but not limited to: 1. the date of the event; 2. a description what information was breached and how the information was breached; 3. how the event was discovered; and 4. the number of total consumers in the state affected by the event. The licensee provides notice of the security breach to consumers residing in the State and whose information was affected by the breach.

Level Texas Covered Entities	Implementation Requirements
Level Texas Covered Entities Implementation:	Organizations or persons that conduct business in Texas and own or license computerized data that includes sensitive personal information disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by unauthorized persons. The disclosure is made as quickly as possible, except at the request of a law enforcement agency that determines notification will impede a criminal investigation, or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system. If the individual is a resident of a state that requires a person or entity to provide notice of a breach of system security, notice of the breach of system security may be provided in accordance with that state's law. A person or entity may give notice by providing: 1. Written notice at the last known address; 2. Electronic notice, if the notice is provided in accordance with 15 U.S.C. Section 7001; or 3. If the person or entity required to give notice demonstrates that the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the person or entity does not have sufficient contact information, the notice may be given by: i. Electronic mail, if the person or entity has electronic mail addresses for the affected persons; ii. Conspicuous posting of the notice on the person's or entity's website; iii. Notice published in, or broadcast on, major statewide media; or iv. Notwithstanding the methods described above, a person or entity who maintains their own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under this section complies with this section if the person or entity notifies affected persons in accordance with that policy. If a person or entity is required by this section to notify more than 10,000 persons of a breach of system security at one time, the person or entity also notifies each consumer reporting agency, as defined by 15 U.S.C. Section 1681a, that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices. The person or entity provides the notice required by this subsection without unreasonable delay. Organizations incorporate procedures in their security and privacy incident response programs to assist with investigations conducted by TX state and local registrars or their representatives, when it is believed a person or persons intentionally or knowingly supplies false information, or intentionally or knowingly creates a false record, or directs another person to supply false information or create a false record, for use in the preparation of a certificate, record or report, or amendment covered under THSC Title 3, as provided by THSC § 195.002 thru 195.005. Private psychiatric (mental) hospitals, crisis stabilization units and other mental health facilities incorporate procedures in their security and privacy incident response programs to assist with state investigations, including the release of otherwise confidential information related to the investigation, as required under THSC § 577.

Level Title 23 NYCRR Part 500	Implementation Requirements

Level Title 23 NYCRR Part 500 Implementation:	The organization must notify the superintendent of financial services for the state of New York within 72 hours from a determination that a cybersecurity event has occurred that is either of the following: 1. Cybersecurity events impacting the organization that require notice to be provided to any government body, self-regulatory agency or any other supervisory body; or 2. Cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the organization.

Control Reference: 11.b Reporting Security Weaknesses

Control Specification:	All employees, contractors, and third-party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.
Factor Type:	Organizational
Topics:	Awareness and Training; Incident Response; Personnel; Third-parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 2 Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	All employees, contractors and third-party users report incident and event information, including violations of workforce rules of behavior and acceptable use agreement, to their management and/or directly to their service provider as quickly as possible in order to prevent information security incidents. The reporting mechanism is easy to use, widely accessible, and available to all employees. Employees, contractors and third-party users are informed (including but not limited to policies and procedures and incident response training) that they do not, in any circumstances, attempt to prove a suspected weakness.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC2.3 AICPA 2017 P6.5 CMMC v1.0 IR.2.093-1 CMSRs v3.1 IR-06 (HIGH; MOD) CMSRs v3.1 PL-04 (HIGH; MOD) CMSRs v3.1 SI-02 (HIGH; MOD) CSA CCM v3.0.1 SEF-03 FedRAMP IR-4 FedRAMP IR-6 FedRAMP PL-4 FedRAMP SI-2 FFIEC IS v2016 A.8.5(g) IRS Pub 1075 v2016 9.3.12.3 IRS Pub 1075 v2016 9.3.17.2 IRS Pub 1075 v2016 9.3.8.6

	ISO/IEC 27002:2013 16.1.3 ISO/IEC 27799:2016 16.1.3 MARS-E v2 IR-6 MARS-E v2 PL-4 MARS-E v2 SI-2 NIST Cybersecurity Framework v1.1 PR.AT-1 NIST Cybersecurity Framework v1.1 RS.CO-2 NRS 603A.215.1 PCI DSS v3.2.1 12.10.4 PMI DSP Framework DE-4

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to FTC Red Flags Rule Subject to NIST SP 800-53 R4 (Supplemental)
Level 2 Implementation:	Level 1 plus: All employees, contractors and third-party users report potential weaknesses that may lead to organization or system breaches, or lead to identity theft for the following categories: 1. alerts, notifications, or other warnings received from third-parties, state or federal agencies or service providers, such as fraud detection services; 2. the presentation of suspicious documents associated with an individual's account; 3. the presentation of suspicious covered information (e.g., an address change that is inconsistent with existing information); 4. the unusual use of, or other suspicious activity related to, an individual's account; and 5. notice from customers, law enforcement authorities, or other persons regarding possible weaknesses in connection with accounts held by the organization.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(3) 16 CFR Part § 681 Appendix A II(c) AICPA 2017 CC2.3 FFIEC IS v2016 A.8.1(m) FFIEC IS v2016 A.8.5(g) ISO/IEC 27002:2013 16.1.3 ISO/IEC 27799:2016 16.1.3 NIST Cybersecurity Framework v1.1 ID.RA-1 NIST Cybersecurity Framework v1.1 RS.AN-5 NIST SP 800-53 R4 IR-6(2)[S]{0} PMI DSP Framework DE-4

Objective Name: 11.02 Management of Information Security Incidents and Improvements

Control Objective:	To ensure a consistent and effective approach to the management of information security incidents.

Control Reference: 11.c Responsibilities and Procedures

Control Specification:	Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Awareness and Training; Contingency Planning; Documentation and Records; Incident Response; IT Organization and Management Roles and Responsibilities; Policies and Procedures

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 2 Subject to CMMC Level 5 Subject to FTC Red Flags Rule Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Privacy) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to State of Massachusetts Data Protection Act Subject to Texas Health and Safety Code
Level 1 Implementation:	The organization implements a formal incident response program, which includes the definition of specific phases for incident response. The organization implements an incident handling capability for security incidents that includes detection and analysis (including forensics), containment, eradication, and recovery (including public relations and reputation management). A program of business processes and technical measures is established to triage security-related events and handle different types of information security incidents including: 1. information system failures and loss of service; 2. malicious code; 3. denial of service; 4. errors resulting from incomplete or inaccurate business data; 5. breaches of confidentiality and integrity; 6. disclosures of unprotected health information; 7. misuse of information systems; 8. identity theft; and 9. unauthorized wireless access points. In addition to normal contingency plans, the program also covers:

	1. analysis and identification of the cause of the incident; 2. containment; 3. restoration and follow-up strategies; 4. increased monitoring of system use; 5. planning and implementation of corrective action to prevent recurrence including: i. changing of password or security codes; ii. changing of devices that permit access to the organization's systems or network; iii. modifying or terminating an account of individuals involved directly or indirectly by the incident (e.g., employees, third-parties, contractors, customers); and 6. assigning a single point of contact for the organization responsible for sharing information and coordinating responses and that has the authority to direct actions required in all phases of the incident response process. The organization tests and/or exercises its incident response capability regularly.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(3) 16 CFR Part § 681 Appendix A IV(a) 16 CFR Part § 681 Appendix A IV(b) 16 CFR Part § 681 Appendix A IV(c) 16 CFR Part § 681 Appendix A IV(d) 16 CFR Part § 681 Appendix A IV(e) 16 CFR Part § 681 Appendix A IV(f) 16 CFR Part § 681 Appendix A IV(g) 16 CFR Part § 681 Appendix A IV(h) 16 CFR Part § 681 Appendix A IV(i) 201 CMR 17.03(2)(j) AICPA 2017 CC7.5 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMMC v1.0 IR.2.094-0 CMMC v1.0 IR.2.096-0 CMMC v1.0 IR.5.110-0 COBIT 5 DS5.6 COBIT 5 DSS02.01 COBIT 5 DSS02.04 COBIT 5 DSS02.05 CRR v2016 IM:G2.Q3 CRR v2016 IM:G2.Q5 CRR v2016 IM:G5.Q1 CRR v2016 IM:MIL5.Q1 CSA CCM v3.0.1 IVS-13 CSA CCM v3.0.1 SEF-02 FFIEC IS v2016 A.8.5(c) FFIEC IS v2016 A.8.5(e) FFIEC IS v2016 A.8.5(f) FFIEC IS v2016 A.8.6(a) FFIEC IS v2016 A.8.6(c) FFIEC IS v2016 A.8.6(d) FFIEC IS v2016 A.8.6(e) FFIEC IS v2016 A.8.6(f) FFIEC IS v2016 A.8.6(h) FFIEC IS v2016 A.8.6(i) ISO/IEC 27002:2013 13.1.1 ISO/IEC 27002:2013 13.2.1 ISO/IEC 27002:2013 16.1.1 ISO/IEC 27002:2013 16.1.5 ISO/IEC 27799:2016 16.1.1 ISO/IEC 27799:2016 16.1.5 NIST Cybersecurity Framework v1.1 PR.IP-10 NIST Cybersecurity Framework v1.1 PR.IP-9 NIST Cybersecurity Framework v1.1 RC.CO-1 NIST Cybersecurity Framework v1.1 RC.CO-2 NIST Cybersecurity Framework v1.1 RS.AN-3 NIST Cybersecurity Framework v1.1 RS.AN-4 NIST Cybersecurity Framework v1.1 RS.CO-4 NIST Cybersecurity Framework v1.1 RS.MI-1

	NIST Cybersecurity Framework v1.1 RS.MI-2 NIST Cybersecurity Framework v1.1 RS.RP-1 NIST SP 800-53 R4 IR-4a[HML]{2} NIST SP 800-53 R4 SE-2[P]{1} NIST SP 800-53 R4 SI-3(10)b[S]{0} NY DOH SSP v3.1 IR-3.IS1[HM]-1 PCI DSS v3.2.1 11.1.2 PMI DSP Framework RS-1 PMI DSP Framework RS-4

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to 23 NYCRR 500 Subject to CA Civil Code § 1798.81.5 Subject to CMMC Level 3 Subject to NIST 800-171 Derived Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to the State of Nevada Security of Personal Information Requirements
Level 2 Implementation:	Level 1 plus: Audit trails and similar evidence are collected and secured, as appropriate, for: 1. internal problem analysis; 2. use as forensic evidence in relation to a potential breach of contract, regulatory requirement or in the event of civil or criminal proceedings (e.g., under computer misuse or data protection legislation); and 3. negotiating for compensation from software and service suppliers. A log of any occurring incident is maintained, and this log is to be submitted annually to the appropriate parties (e.g., a state, regional, or national regulatory agency. Action to recover from security breaches and correct system failures is carefully and formally controlled. The procedures ensure that: 1. only clearly identified and authorized personnel are allowed access to live systems and data; 2. all emergency actions taken are documented in detail; 3. damage is minimized through the containment of the incident, restoration of systems, and preservation of data and evidence; 4. emergency action is reported to management and reviewed in an orderly manner; and

	5. the integrity of business systems and controls is confirmed with minimal delay; and 6. stakeholders are notified immediately when a safe and secure environment has been restored. The organization disseminates incident response policy and procedures to appropriate elements within the organization. Responsible parties within the organization on a pre-defined frequency review incident response policy and procedures. The organization updates incident response policy and procedures when organizational review indicates updates are required. The organization responds to incidents in accordance with the documented procedures, which includes, but is not limited to, the following: 1. collecting evidence as soon as possible after the occurrence (see 11.e); 2. conducting information security forensic analysis, as required (see 11.e); 3. escalation, as required; 4. ensuring that all involved response activities are properly logged for later analysis; 5. communicating the existence of the information security incident or any relevant details thereof to other internal and external people or organizations with a need to know; 6. dealing with information security weakness(es) found to cause or contribute to the incident; and 7. once the incident has been successfully addressed, formally closing and recording it. The organization coordinates incident response testing with organization elements responsible for related plans. Incident Response Testing and Exercises procedures include: 1. defining incident response tests/exercises, including automated mechanisms; 2. defining the frequency of incident response tests/exercises; 3. testing the incident response capability for the information system using organization-defined tests/exercises in accordance with organization-defined frequency; and 4. documenting the results of incident response tests/exercises. In addition to reporting of information security events and weaknesses, the monitoring of systems, alerts, and vulnerabilities is used to detect information security incidents. The organization tests and/or exercises the incident response capability for the information system within every 365 days using reviews, analyses, and simulations to determine the incident response effectiveness, and produces an after-action report to improve existing processes, procedures, and policies. Such testing includes personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team. A formal test need not be conducted if the organization actively exercises its response capability using real incidents. The incident management plan is reviewed and updated annually.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC3.1 AICPA 2017 CC7.3 AICPA 2017 CC7.4 AICPA 2017 CC7.5 AICPA 2017 P6.3 CIS CSC v7.1 19.7 CMMC v1.0 IR.3.099-0 CMSRs v3.1 IR-01 (HIGH; MOD) CMSRs v3.1 IR-03 (HIGH; MOD)

	CMSRs v3.1 IR-03(02) (HIGH; MOD) CMSRs v3.1 IR-08 (HIGH; MOD) CMSRs v3.1 SE-02 (HIGH; MOD) CRR v2016 IM:G1.Q2 CRR v2016 IM:G2.Q8 CRR v2016 IM:G2.Q9 CRR v2016 IM:G4.Q1 CRR v2016 IM:G5.Q1 CRR v2016 IM:MIL3.Q4 CRR v2016 IM:MIL4.Q1 CRR v2016 IM:MIL4.Q3 FedRAMP IR-1 FedRAMP IR-3 FedRAMP IR-3(2) FedRAMP IR-8 FFIEC IS v2016 A.6.21(c) FFIEC IS v2016 A.8.5(h) FFIEC IS v2016 A.8.6(a) FFIEC IS v2016 A.8.6(b) FFIEC IS v2016 A.8.6(d) FFIEC IS v2016 A.8.6(e) FFIEC IS v2016 A.8.6(f) FFIEC IS v2016 A.8.6(g) IRS Pub 1075 v2016 10.3 IRS Pub 1075 v2016 9.3.8.1 IRS Pub 1075 v2016 9.3.8.3 IRS Pub 1075 v2016 9.3.8.8 ISO/IEC 27002:2013 16.1.5 ISO/IEC 27799:2016 16.1.5 ISO/IEC 27799:2016 7.10.2.1 MARS-E v2 IR-1 MARS-E v2 IR-3 MARS-E v2 IR-3(2) MARS-E v2 IR-8 MARS-E v2 SE-2 NIST 800-171 r2 3.6.3-0 NIST Cybersecurity Framework v1.1 DE.AE-3 NIST Cybersecurity Framework v1.1 ID.SC-5 NIST Cybersecurity Framework v1.1 PR.AT-1 NIST Cybersecurity Framework v1.1 PR.IP-10 NIST Cybersecurity Framework v1.1 PR.IP-9 NIST Cybersecurity Framework v1.1 RS.CO-2 NIST Cybersecurity Framework v1.1 RS.CO-3 NIST Cybersecurity Framework v1.1 RS.CO-4 NIST Cybersecurity Framework v1.1 RS.IM-2 NIST Cybersecurity Framework v1.1 RS.RP-1 NIST SP 800-53 R4 IR-3(2)[HM]{0} NIST SP 800-53 R4 IR-3[HM]{0} NIST SP 800-53 R4 IR-8a[HML]{1} NIST SP 800-53 R4 IR-8a[HML]{3} NIST SP 800-53 R4 IR-8a[HML]{7} NIST SP 800-53 R4 IR-8a[HML]{8} NIST SP 800-53 R4 IR-8b[HML]{0} NIST SP 800-53 R4 IR-8c[HML]{0} NIST SP 800-53 R4 SA-12(12)[S]{0} NIST SP 800-53 R4 SI-3(6)b[S]{1} NRS 603A.215.1 NY DOH SSP v3.1 IR-1[M]-2 NY DOH SSP v3.1 IR-1b1[M]-0 NY DOH SSP v3.1 IR-1b2[M]-0 NY DOH SSP v3.1 IR-2.IS1[HML]-0 PCI DSS v3.2.1 12.10.1 PCI DSS v3.2.1 12.10.2 PCI DSS v3.2.1 12.10.4 PMI DSP Framework RC-1 PMI DSP Framework RC-2 PMI DSP Framework RS-1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions

	Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to Banking Requirements Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: The organization: 1. develops an incident response plan that: i. provides the organization with a roadmap for implementing its incident response capability; ii. describes the structure and organization of the incident response capability; iii. provides a high-level approach for how the incident response capability fits into the overall organization; iv. meets the unique requirements of the organization, which relate to mission, size, structure, and functions; v. defines reportable incidents; vi. provides metrics for measuring the incident response capability within the organization; vii. defines the resources and management support needed to effectively maintain and mature an incident response capability; and viii. is reviewed and approved by designated officials within the organization; 2. distributes copies of the incident response plan to incident response personnel and organizational elements; 3. reviews the incident response plan within every 365 days; 4. revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and 5. communicates incident response plan changes to incident response personnel and organizational elements. The organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The incident response support resource is an integral part of the organization's incident response capability. The organization tracks and documents information system security incidents on an ongoing basis. The organization promptly reports incident information to appropriate authorities. The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

	Weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents. The organization communicates with outside parties regarding the incident. This includes reporting incidents to organizations such as the Federal Computer Incident Response Center (FedCIRC) and the CERT Coordination Center (CERT/CC), contacting law enforcement, and fielding inquiries from the media. The objectives for information security incident management are agreed to with management, and it are ensured that those responsible for information security incident management understand the organization's priorities for handling information security incidents. The organization employs automated mechanisms to increase the availability of incident response related information and support.
Level 3 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMSRs v3.1 IR-06 (HIGH; MOD) CMSRs v3.1 IR-07 (HIGH; MOD) CRR v2016 IM:G2.Q1 CSA CCM v3.0.1 SEF-03 FedRAMP IR-4 FedRAMP IR-6 FedRAMP IR-7 FFIEC IS v2016 A.8.5(f) FFIEC IS v2016 A.8.6(f) IRS Pub 1075 v2016 9.3.8.6 IRS Pub 1075 v2016 9.3.8.7 ISO/IEC 27002:2013 16.1.3 ISO/IEC 27002:2013 16.1.5 ISO/IEC 27799:2016 16.1.3 ISO/IEC 27799:2016 16.1.5 MARS-E v2 IR-6 MARS-E v2 IR-7 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 PR.IP-9 NIST Cybersecurity Framework v1.1 RS.CO-1 NIST Cybersecurity Framework v1.1 RS.CO-2 NIST Cybersecurity Framework v1.1 RS.CO-3 NIST Cybersecurity Framework v1.1 RS.CO-5 NIST Cybersecurity Framework v1.1 RS.MI-2 NIST SP 800-53 R4 IR-7[HML]{0} NY DOH SSP v3.1 IR-7[M]-0 PMI DSP Framework DE-5 PMI DSP Framework RS-1

Level CIS Implementation Requirements

Level CIS Implementation:	Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats. Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.

Level CMMC Implementation Requirements

Level CMMC Implementation:	The organization establishes and maintains a Cyber Incident Response Team (CIRT) that can investigate an issue physically or virtually at any location within 24 hours.

Level CMS Implementation Requirements

Level CMS Implementation:	The organization employs automated mechanisms to assist in the tracking of security incidents.

	The organization distributes copies of the incident response plan to: 1. CMS Chief Information Security Officer; 2. CMS Chief Information Officer; 3. Information System Security Officer; 4. CMS Office of the Inspector General/Computer Crimes Unit; 5. All personnel within the organization Incident Response Team; 6. All personnel within the PII Breach Response Team; and 7. All personnel within the organization Operations Centers. The organization communicates incident response plan changes to the organizational elements listed above for distribution.
Level Community Supplemental Reqs 02	**Implementation Requirements**
Level Community Supplemental Reqs 02 Implementation:	The organization develops incident detection and response procedures that include: i) identifying and alerting on anomalous network traffic (from lessons learned from investigations, variances to normal traffic models, anomalous behavior and other attack patterns identified by threat-hunting/data analysis); and ii) analyzing network packets to support investigation and forensics activities. The organization develops incident response plans that include the roles and responsibilities of both internal resources and third-party service providers, including details on when third-party service providers are required to assist in investigation and response activities. The organization develops a procedure to quarantine compromised systems and systems suspected of compromise to preserve evidence for investigation and allows such systems only basic connectivity to other systems for response purposes. For host-based quarantine methods, the organization implements a process to determine whether the method failed to achieve intended results and implements additional controls to isolate or remove from the network. The organization employs the capability to acquire system data in near real-time (remotely and directly) for deep forensic analysis. The organization employs the capability to actively search all deployed endpoints to readily identify threat indicators (e.g., from investigations or separate intelligence source). The organization keeps compromised systems in quarantine until the incident is fully remediated. The organization is inclined towards re-imaging a compromised system when there has been confirmed execution of potentially malicious code; otherwise, the organization uses caution when cleaning such systems to ensure malicious code is fully eradicated.
Level FedRAMP	**Implementation Requirements**
Level FedRAMP Implementation:	The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel. The organization agency takes an appropriate response to information spills by: 1. identifying the specific information involved in the information system contamination;

	2. alerting authorized incident response personnel of the information spill using a method of communication not associated with the spill; 3. isolating the contaminated information system or system component; 4. eradicating the information from the contaminated information system or component; and 5. identifying other information systems or system components that may have been subsequently contaminated. The organization implements the following in response to information spills: 1. assigns organization-defined personnel or roles with responsibility for responding to information spills; 2. provides information spillage response training; 3. ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions; and 4. employs security safeguards for personnel exposed to information not within assigned access authorizations. The organization implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, which include the following requirements: 1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; 2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured. The organization has developed and implemented alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation:	The agency must track and document all physical and information system security incidents potentially affecting the confidentiality of FTI. The agency must not wait to conduct an internal investigation to determine if FTI was involved in an unauthorized disclosure or data breach. If FTI may have been involved, the agency must contact TIGTA and the IRS immediately. The agency will cooperate with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident. The organization exercises its response to unauthorized FTI access and reporting of unauthorized FTI access to IRS and TIGTA. Agencies must perform tabletop exercises using scenarios that include a breach of FTI and test the agency's incident response policies and procedures. All employees and contractors with significant FTI incident response capabilities, including technical personnel responsible for maintaining consolidated data centers and off-site storage, must be included in tabletop exercises. Each tabletop exercise must produce an after-action report to improve existing processes, procedures, and policies.

	The agency provides an incident response support resource that offers advice and assistance to users of the federal tax information and any information system containing federal tax information for the handling and reporting of security incidents. The support resource is an integral part of the agency's incident response capability. The agency develops, documents, and maintains a current incident response plan that describes the structure and organization of the incident response capability and includes incident response procedures specific to FTI, including any data warehousing environment that contains FTI. The agency must respond to information spills by: 1. Identifying the specific information involved in the information system contamination; 2. Alerting authorized incident response personnel of the information spill using a method of communication not associated with the spill; 3. Isolating the contaminated information system or system component; 4. Eradicating the information from the contaminated information system or component; and 5. v. Identifying other information systems or system components that may have been subsequently contaminated.

Level HIPAA Implementation Requirements

Level HIPAA Implementation:	For the purposes of determining when external parties must be notified, the organization treats security events as discovered on the first day in which the security event is or would have been known by the organization through exercising reasonable due diligence.

Level HIX Implementation Requirements

Level HIX Implementation:	The organization responds to information spills by: 1. Requiring personnel to report suspected incidents to the organizational incident response capability within the timeframe established in the current Administering Entity (AE) organization Incident Handling Procedure and ACA incident handling reporting process, available at https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/; 2. Identifying the specific information involved in the improper or potentially improper information disclosure; 3. Alerting authorized incident response personnel of the information spill using a method of communication not associated with the spill; 4. Identifying other information systems or system components on which the information may have been subsequently improperly or potentially improperly shared with or disclosed to; and 5. Removing and destroying the information from the contaminated information system, component or individual not authorized to handle such information.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	The organization tracks and documents all physical, information security, and privacy incidents. The organization investigates suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action.

Level SCIDSA Implementation Requirements

Level SCIDSA Implementation:	Upon notification of a cybersecurity event, the licensee conducts a prompt and thorough investigation of the event.

Control Reference: 11.d Learning from Information Security Incidents

Control Specification:	There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Awareness and Training; Incident Response; IT Organization and Management Roles and Responsibilities

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 2 Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to Texas Health and Safety Code
Level 1 Implementation:	The information gained from the evaluation of information security incidents is used to identify recurring or high-impact incidents and update the incident response and recovery strategy. Mechanisms are put in place to monitor and quantify the types, volumes, and costs of information security incidents.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMMC v1.0 IR.2.097-0 CRR v2016 IM:G2.Q4 CRR v2016 IM:G3.Q3 CSA CCM v3.0.1 SEF-05 ISO/IEC 27002:2013 16.1.6 ISO/IEC 27799:2016 16.11.6 NIST Cybersecurity Framework v1.1 DE.AE-1 NIST Cybersecurity Framework v1.1 DE.AE-2 NIST Cybersecurity Framework v1.1 DE.AE-4 NIST Cybersecurity Framework v1.1 RC.IM-1 NIST Cybersecurity Framework v1.1 RC.IM-2 NIST Cybersecurity Framework v1.1 RC.RP-1 NIST Cybersecurity Framework v1.1 RS.AN-2 NIST Cybersecurity Framework v1.1 RS.IM-1 NIST Cybersecurity Framework v1.1 RS.IM-2 NIST Cybersecurity Framework v1.1 RS.RP-1 NIST SP 800-53 R4 IR-8a[HML]{6} PMI DSP Framework RC-3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions

	Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to 23 NYCRR 500 Subject to CMMC Level 2 Subject to CMMC Level 4 Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to HIPAA Security Rule Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST 800-171 Basic Level Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to State of Massachusetts Data Protection Act Subject to Supplemental Requirements Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The organization: 1. coordinates incident handling activities with contingency planning activities; and 2. incorporates lessons learned from ongoing incident handling activities and industry developments into incident response procedures, training and testing exercises, and implements the resulting changes accordingly. Components include: 1. policy (setting corporate direction) and procedures defining roles and responsibilities; 2. incident handling procedures (business and technical); 3. communication; 4. reporting and retention; and 5. references to vulnerability management program that includes network tools for IPS, IDS, forensics, vulnerability assessments and validation.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.308(a)(6)(i) HIPAA.SR-0 45 CFR Part § 164.308(a)(6)(ii) HIPAA.SR-0 AICPA 2017 CC7.4 AICPA 2017 CC7.5 CMMC v1.0 IR.2.092-1 CMMC v1.0 IR.2.092-2 CMMC v1.0 IR.4.100-2 CMSRs v3.1 IR-04 (HIGH; MOD) CMSRs v3.1 IR-04(01) (HIGH; MOD) CMSRs v3.1 IR-04(04) (HIGH) CMSRs v3.1 IR-05 (HIGH; MOD) CMSRs v3.1 IR-05(01) (HIGH) CRR v2016 IM:G1.Q3

	CRR v2016 IM:G2.Q4 CRR v2016 IM:G2.Q7 CRR v2016 IM:G3.Q3 CRR v2016 IM:G5.Q2 CRR v2016 IM:G5.Q3 CRR v2016 IM:MIL3.Q4 CRR v2016 IM:MIL4.Q1 CRR v2016 IM:MIL5.Q2 FedRAMP IR-4 IRS Pub 1075 v2016 10.3 IRS Pub 1075 v2016 9.3.8.4 MARS-E v2 IR-4 MARS-E v2 IR-4(1) NIST 800-171 r2 3.6.1-1 NIST 800-171 r2 3.6.1-2 NIST Cybersecurity Framework v1.1 DE.AE-2 NIST Cybersecurity Framework v1.1 DE.AE-3 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 RC.CO-1 NIST Cybersecurity Framework v1.1 RC.CO-2 NIST Cybersecurity Framework v1.1 RC.IM-1 NIST Cybersecurity Framework v1.1 RC.IM-2 NIST Cybersecurity Framework v1.1 RC.RP-1 NIST Cybersecurity Framework v1.1 RS.AN-1 NIST Cybersecurity Framework v1.1 RS.AN-3 NIST Cybersecurity Framework v1.1 RS.CO-3 NIST Cybersecurity Framework v1.1 RS.CO-4 NIST Cybersecurity Framework v1.1 RS.IM-1 NIST Cybersecurity Framework v1.1 RS.IM-2 NIST Cybersecurity Framework v1.1 RS.MI-1 NIST Cybersecurity Framework v1.1 RS.MI-2 NIST SP 800-53 R4 CP-2c[HML]{0} NIST SP 800-53 R4 IR-4a[HML]{1} NIST SP 800-53 R4 IR-4b[HML]{0} NIST SP 800-53 R4 IR-4c[HML]{0} NIST SP 800-53 R4 IR-8d[HML]{0} NIST SP 800-53 R4 SA-15(7)d[S]{0} NIST SP 800-53 R4 SI-3(6)b[S]{2} NRS 603A.215.1 NY DOH SSP v3.1 CP-2c[M]-0 NY DOH SSP v3.1 IR-1a2[M]-0 NY DOH SSP v3.1 IR-4(3).IS1[H]-0 NY DOH SSP v3.1 PM-15a[M]-4 PCI DSS v3.2.1 12.10.6 PMI DSP Framework RC-3 SR v6.4 34-0 SR v6.4 34a-0

Level CMS Implementation Requirements

Level CMS Implementation:	The organization implements an incident handling capability using the current CMS Incident Handling and Breach Notification Standard and Procedures. Relevant information related to a security incident is documented according to the current CMS Incident Handling and Breach Notification Standard and Procedures. The organization employs automated mechanisms to assist in the collection and analysis of incident information. The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

Level FedRAMP Implementation Requirements

Level FedRAMP Implementation:	The organization employs automated mechanisms to assist in the collection and analysis of incident information.

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation:	The organization provides specific incident response guidance relative to data incidents involving FTI. Once the incident has been addressed, the agency will conduct a post-incident review to ensure the incident response policies and procedures provide adequate guidance. Complete SPR section 9.11.5

Level NYDOH Implementation Requirements	
Level NYDOH Implementation:	The organization (i) implements an incident handling capability (i.e., system incident response plan) using the current RMH, Chapter 08: Incident Response; (ii) coordinates incident handling activities with contingency planning activities; and (iii) incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises and implements the resulting changes accordingly.

Control Reference: 11.e Collection of Evidence

Control Specification:	Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented in support of potential legal action in accordance with the rules for evidence in the relevant jurisdiction(s).
Factor Type:	Organizational
Topics:	Documentation and Records; Incident Response; Requirements (Legal and Contractual); Services and Acquisitions

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to Texas Health and Safety Code
Level 1 Implementation:	The organization collects, retains, and presents evidence to support legal action (either civil or criminal). The evidence that is collected, retained, and presented is done in accordance with the laws of the relevant jurisdiction(s).
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 16 CFR Part § 681 Appendix A IV(a) CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CRR v2016 IM:G2.Q9 CSA CCM v3.0.1 SEF-04 ISO/IEC 27002:2013 16.1.7 ISO/IEC 27799:2016 16.1.7 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 RS.AN-3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CMMC Level 5 Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to PCI Compliance Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: Internal procedures are developed, documented and followed when collecting and presenting evidence for the purposes of disciplinary action handled within an organization. To achieve admissibility of the evidence, the organization ensures that their information systems comply with any published standard or code of practice for the production of admissible evidence. The weight of evidence provided complies with any applicable requirements. To achieve weight of evidence, the quality and completeness of the controls used to correctly and consistently protect the evidence (i.e., process control evidence) throughout the period that the evidence to be recovered was stored and processed are demonstrated by a strong evidence trail established with the following conditions: 1. for paper documents: the original is kept securely with a record of the individual who found the document, where the document was found, when the document was found, and who witnessed the discovery; any investigation ensures that originals are not tampered with. 2. for information on computer media: mirror images or copies (depending on applicable requirements) of any removable media, information on hard disks or in memory are taken to ensure availability; the log of all actions during the copying process is kept, and the process is witnessed; the original media and the log (if this is not possible, at least one mirror image or copy) are kept securely and untouched. Any forensics work is only performed on copies of the evidential material. The integrity of all evidential material is protected. Copying of evidential material is supervised by trustworthy personnel, and information on when and where the copying process was executed, who performed the copying activities, and which tools and programs have been utilized is logged.

	Organizations incorporate appropriate forensic handling procedures. Forensics can be outsourced or handled in-house. Any type of forensics requires training, staff and processes for maintaining a proper chain of evidence. Upon notification, customers and/or other external business partners impacted by a security breach are given the opportunity to participate, as is legally permissible, in the forensic investigation.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) CMMC v1.0 IR.5.106-0 CMSRs v3.1 IR-04 (HIGH; MOD) CRR v2016 IM:G2.Q8 CRR v2016 IM:G2.Q9 CRR v2016 IM:MIL3.Q2 CSA CCM v3.0.1 SEF-04 FedRAMP IR-4 FFIEC IS v2016 A.8.1(b) IRS Pub 1075 v2016 9.3.8.4 ISO/IEC 27002:2013 16.1.1 ISO/IEC 27002:2013 16.1.7 ISO/IEC 27799:2016 16.1.1 ISO/IEC 27799:2016 16.1.7 MARS-E v2 IR-4 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST Cybersecurity Framework v1.1 RS.AN-3 NIST SP 800-53 R4 IR-10[S]{1} NIST SP 800-53 R4 IR-10[S]{2} NRS 603A.215.1 NY DOH SSP v3.1 AU-2.IS4[M]-0 PCI DSS v3.2.1 A1.4
Level Cloud Service Providers	**Implementation Requirements**
Level Cloud Service Providers Implementation:	Upon notification, customers and/or other external business partners impacted by a security breach are given the opportunity to participate, as is legally permissible, in the forensic investigation.
Level Community Supplemental Reqs 02	**Implementation Requirements**
Level Community Supplemental Reqs 02 Implementation:	The organization deploys a solution to monitor and retain detailed endpoint telemetry that: i) records details such as trace of process execution (e.g. file paths, libraries called, sockets opened, files opened/written), network connections, file input/output, and registry changes; ii) can implement customized detection rules to complement endpoint preventative controls and address gaps in other solutions (e.g. banning files/hashes, network connections, processes execution); and iii) aggregates and makes data available to others for building detection rules and investigating incidents. The organization documents details on flow of sensitive data to the individual systems, including the details on system type (e.g., manufacturer, operating system), roles (e.g., database, file server), and network location (e.g., subnet, IP address).
Level NYDOH	**Implementation Requirements**
Level NYDOH Implementation:	The organization (i) preserves evidence related to security incidents through technical means, including secured storage of evidence media and “write” protection of evidence media; (ii) uses sound forensics processes and utilities that support legal requirements; and (iii) determines and follows a chain of custody for forensic evidence.

	When subject to a legal investigation (e.g., Insider Threat), audit records must be maintained until released by the investigating authority. When subject to a legal investigation (e.g., of an insider threat), continuous monitoring records must be maintained until released by the investigating authority.

Level PCI Implementation Requirements	
Level PCI Implementation:	A service provider protects each organization's hosted environment and data by enabling a process to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.

Control Category: 12.0 - Business Continuity Management

Objective Name: 12.01 Information Security Aspects of Business Continuity Management

Control Objective:	To ensure that strategies and plans are in place to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Control Reference: 12.a Including Information Security in the Business Continuity Management Process

Control Specification:	A managed program and process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.
Factor Type:	Organizational
Topics:	Contingency Planning; Documentation and Records; IT Organization and Management Roles and Responsibilities; Media and Assets; Personnel; Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to Texas Health and Safety Code
Level 1 Implementation:	The program and process bring together the following key elements of business continuity management: 1. identifying all the assets involved in critical business processes; 2. considering the purchase of suitable insurance, which may form part of the overall business continuity process, as well as being part of operational risk management; 3. ensuring the safety of personnel and the protection of information assets and organizational property; and 4. formulating and documenting business continuity plans addressing information security requirements in line with the agreed business continuity strategy (see 12.c).
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC9.1 CMSRs v3.1 CP-02 (HIGH; MOD) CMSRs v3.1 CP-02(08) (HIGH; MOD) CRR v2016 EDM:G3.Q1 CRR v2016 SCM:G1.Q1 CRR v2016 SCM:MIL2.Q1 CRR v2016 SCM:MIL2.Q2 CRR v2016 SCM:MIL2.Q4 CSA CCM v3.0.1 BCR-09 FedRAMP CP-2 FedRAMP CP-2(8) IRS Pub 1075 v2016 9.3.6.2

	ISO/IEC 27002:2013 17.1.2 ISO/IEC 27799:2016 17.1.2 MARS-E v2 CP-2 NIST Cybersecurity Framework v1.1 ID.AM-5 NIST Cybersecurity Framework v1.1 PR.IP-11 NIST Cybersecurity Framework v1.1 PR.IP-9 NIST SP 800-53 R4 AU-1[HML]{0}

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to 23 NYCRR 500 Subject to Banking Requirements Subject to CRR V2016 Subject to FedRAMP Certification Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The program and process bring together the following key elements of business continuity management: 1. identifying critical information system assets supporting organizational missions and functions; 2. understanding the risks the organization is facing in terms of likelihood and impact in time, including an identification and prioritization of critical business processes; 3. understanding the impact which interruptions caused by information security incidents are likely to have on the business (it is important that solutions are found that will handle incidents causing smaller impact, as well as serious incidents that could threaten the viability of the organization), and establishing the business objectives of information assets; 4. implementing additional preventive detective controls for the critical assets identified to mitigate risks to the greatest extent possible; 5. identifying financial, organizational, technical, and environmental resources to address the identified information security requirements; 6. testing and updating, at a minimum, a section of the plans and processes put in place at least annually; 7. ensuring that the management of business continuity is incorporated in the organization's processes and structure; and

	8. assigning responsibility for the business continuity management process at an appropriate level within the organization.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 CC7.3 AICPA 2017 CC7.4 AICPA 2017 CC7.5 AICPA 2017 CC9.1 CMSRs v3.1 CP-02 (HIGH; MOD) CMSRs v3.1 CP-02(08) (HIGH; MOD) CMSRs v3.1 PM-09 (HIGH; MOD) CRR v2016 AM:G2.Q1 CRR v2016 CCM:G1.Q2 CRR v2016 EDM:G3.Q1 CRR v2016 SCM:G1.Q1 CRR v2016 SCM:G3.Q1 CRR v2016 SCM:G3.Q3 CRR v2016 SCM:MIL3.Q4 CSA CCM v3.0.1 BCR-09 FedRAMP CP-2 FedRAMP CP-2(8) FFIEC IS v2016 A.6.35(a) FFIEC IS v2016 A.6.35(c) IRS Pub 1075 v2016 9.3.6.2 ISO/IEC 27002:2013 17.1.2 ISO/IEC 27799:2016 17.1.2 MARS-E v2 CP-2 MARS-E v2 PM-9 NIST Cybersecurity Framework v1.1 DE.AE-4 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 ID.BE-5 NIST Cybersecurity Framework v1.1 PR.IP-9 NIST SP 800-53 R4 CP-2(8)[HM]{0} NIST SP 800-53 R4 CP-4[HML]{0} NIST SP 800-53 R4 SA-13a[S]{2} NIST SP 800-53 R4 SA-14[S]{2} NY DOH SSP v3.1 CP-2(8)[M]-0

Level HIPAA Implementation Requirements

Level HIPAA Implementation:	The organization implements procedures under the disaster recovery plan (or related plans) to allow facility access in support of restoration activities in emergency-related events.

Control Reference: 12.b Business Continuity and Risk Assessment

Control Specification:	Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Contingency Planning; IT Organization and Management Roles and Responsibilities; Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to FISMA Compliance Subject to HITRUST De-ID Framework Requirements Subject to MARS-E Requirements

	Subject to NIST SP 800-53 R4 (Supplemental) Subject to Texas Health and Safety Code Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	This process identifies the critical business processes. Information security aspects of business continuity are based on identifying events (or sequence of events) that can cause interruptions to the organization's critical business processes (e.g., equipment failure, human errors, theft, fire, natural disasters and acts of terrorism). This is followed by a risk assessment to determine the probability and impact of such interruptions, in terms of time, damage scale and recovery period. Based on the results of the risk assessment, a business continuity strategy is developed to identify the overall approach to business continuity. Once this strategy has been created, endorsement is provided by management, and a plan created and endorsed to implement this strategy.
Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 A1.3 CMSRs v3.1 CP-02 (HIGH; MOD) CMSRs v3.1 CP-02(08) (HIGH; MOD) CRR v2016 EDM:G3.Q1 CRR v2016 SCM:G1.Q1 CRR v2016 SCM:G1.Q2 De-ID Framework v1 Physical and Environmental Security: General FedRAMP CP-2 FedRAMP CP-2(8) IRS Pub 1075 v2016 9.3.6.2 ISO/IEC 27002:2013 17.1.1 ISO/IEC 27002:2013 17.1.2 ISO/IEC 27799:2016 17.1.1 ISO/IEC 27799:2016 17.1.2 MARS-E v2 CP-2 NIST Cybersecurity Framework v1.1 DE.AE-4 NIST Cybersecurity Framework v1.1 ID.BE-2 NIST Cybersecurity Framework v1.1 ID.BE-5 NIST Cybersecurity Framework v1.1 ID.RA-1 NIST Cybersecurity Framework v1.1 ID.RA-3 NIST Cybersecurity Framework v1.1 ID.RA-4 NIST Cybersecurity Framework v1.1 ID.RA-5 NIST Cybersecurity Framework v1.1 ID.RM-3 NIST Cybersecurity Framework v1.1 PR.IP-9 NIST Cybersecurity Framework v1.1 PR.PT-5 NIST SP 800-53 R4 SI-13a[S]{2}

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to CMMC Level 3 Subject to CRR V2016 Subject to HIPAA Security Rule Subject to Joint Commission Accreditation
Level 2 Implementation:	Level 1 plus:

	This process identifies the critical business processes and integrates the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities. The consequences of disasters, security failures, loss of service, and service availability are subject to a business impact analysis. Business continuity risk assessments are carried out annually with full involvement from owners of business resources and processes. This assessment considers all business processes and is not limited to the information assets but includes the results specific to information security. It is important to link the different risk aspects together to obtain a complete picture of the business continuity requirements of the organization. The assessment identifies, quantifies, and prioritizes risks against key business objectives and criteria relevant to the organization, including critical resources, impacts of disruptions, allowable outage times, and recovery priorities.
Level 2 Control Standard Mapping:	45 CFR Part § 164.308(a)(7)(ii)(E) HIPAA.SR-1 45 CFR Part § 164.308(a)(7)(ii)(E) HIPAA.SR-2 AICPA 2017 CC3.3 CMMC v1.0 RM.3.144-1 CMSRs v3.1 PM-08 (HIGH; MOD) CRR v2016 AM:G3.Q1 CRR v2016 AM:G7.Q1 CRR v2016 RM:G2.Q2 CRR v2016 SCM:G1.Q4 CRR v2016 SCM:MIL2.Q4 CRR v2016 SCM:MIL3.Q4 CSA CCM v3.0.1 BCR-09 ISO/IEC 27002:2013 17.1.1 ISO/IEC 27799:2016 17.1.1 MARS-E v2 PM-8 NIST Cybersecurity Framework v1.1 ID.BE-2 NIST Cybersecurity Framework v1.1 ID.BE-4 NIST Cybersecurity Framework v1.1 ID.RA-3 NIST Cybersecurity Framework v1.1 ID.RA-4 NIST Cybersecurity Framework v1.1 ID.RA-5 NIST Cybersecurity Framework v1.1 ID.RM-3

Control Reference: 12.c Developing and Implementing Continuity Plans Including Information Security

Control Specification:	Plans shall be developed and implemented to maintain or restore operations and ensure availability of information, at the required level and in the required time scales, following interruption to, or failure of, critical business processes. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Awareness and Training; Contingency Planning; Documentation and Records; Physical and Facility Security; Policies and Procedures

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to HIPAA Security Rule Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline

	Subject to PCI Compliance Subject to Texas Health and Safety Code
Level 1 Implementation:	A formal, documented contingency planning policy (addressing purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance); and formal, documented procedures (to facilitate the implementation of the contingency planning policy and associated contingency planning controls) are developed, disseminated, and reviewed annually. The business continuity planning process includes the following: 1. implementation of the procedures to allow recovery and restoration of business operations and availability of information in required time-scales; 2. particular attention is given to the assessment of internal and external business dependencies and the contracts in place; 3. documentation of agreed procedures and processes; and 4. testing and updating of at least a section of the plans. The planning process focuses on the required business objectives (e.g., restoring of specific communication services to customers in an acceptable amount of time). The procedures for obtaining necessary electronic covered information during an emergency are defined. The services and resources facilitating this are identified, including staffing, non-information processing resources, as well as fallback arrangements for information processing facilities. Such fallback arrangements may include arrangements with third-parties in the form of reciprocal agreements, or commercial subscription services. The organization coordinates contingency planning activities with incident handling activities. Developed business continuity plans: 1. identify essential missions and business functions and associated contingency requirements; 2. provide recovery objectives, restoration priorities, and metrics; 3. address contingency roles, responsibilities, assigned individuals with contact information; 4. address maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. address eventual, full information system restoration without deterioration of the security measures originally planned and implemented; 6. be reviewed and approved by designated officials within the organization; and 7. be protected from unauthorized disclosure and modification. Continuity and recovery plans are developed and documented to deal with system interruptions and failures caused by malicious code. Business continuity plans include recovering from malicious code attacks, including all necessary data and software back-up and recovery arrangements. Copies of the business continuity plans are distributed to the Information System Security Officer, System Owner, Contingency Plan Coordinator, System Administrator, and Database Administrator (or the organization's functional equivalents). If alternative temporary locations are used, the level of implemented security controls at these locations is to have logical and physical access controls that are equivalent to the primary site, consistent with the HITRUST CSF. The information system implements transaction recovery for systems that are transaction-based.
Level 1	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi)

Control Standard Mapping:	45 CFR Part § 164.308(a)(7)(i) HIPAA.SR-0 45 CFR Part § 164.308(a)(7)(ii)(B) HIPAA.SR-0 45 CFR Part § 164.308(a)(7)(ii)(C) HIPAA.SR-0 CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMSRs v3.1 CP-02 (HIGH; MOD) CMSRs v3.1 CP-02(02) (HIGH) CMSRs v3.1 CP-02(04) (HIGH) CMSRs v3.1 CP-02(05) (HIGH) CMSRs v3.1 CP-10(04) (HIGH) CRR v2016 CCM:G1.Q3 CRR v2016 SCM:G1.Q1 CRR v2016 SCM:G1.Q4 CRR v2016 SCM:G1.Q6 CRR v2016 SCM:G3.Q3 CRR v2016 SCM:MIL2.Q3 CRR v2016 SCM:MIL2.Q4 CRR v2016 SCM:MIL5.Q1 CSA CCM v3.0.1 BCR-09 De-ID Framework v1 Physical and Environmental Security: General FedRAMP CP-1 FedRAMP CP-2 FedRAMP CP-2(2) FedRAMP CP-2(3) FFIEC IS v2016 A.6.35(a) IRS Pub 1075 v2016 9.3.6.2 ISO/IEC 27002:2013 17.1.2 ISO/IEC 27799:2016 17.1.2 MARS-E v2 CP-10(3) MARS-E v2 CP-2 MARS-E v2 CP-2(2) NIST Cybersecurity Framework v1.1 ID.AM-5 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 ID.BE-4 NIST Cybersecurity Framework v1.1 ID.BE-5 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.DS-4 NIST Cybersecurity Framework v1.1 PR.IP-7 NIST Cybersecurity Framework v1.1 PR.IP-9 NIST Cybersecurity Framework v1.1 RC.CO-3 NIST Cybersecurity Framework v1.1 RC.RP-1 NIST Cybersecurity Framework v1.1 RS.CO-1 NIST Cybersecurity Framework v1.1 RS.CO-4 NIST SP 800-53 R4 CP-10(2)[HM]{0} NIST SP 800-53 R4 CP-2a[HML]{2} NIST SP 800-53 R4 CP-2a[HML]{3} NIST SP 800-53 R4 CP-2a[HML]{4} NIST SP 800-53 R4 CP-2b[HML]{0} NY DOH SSP v3.1 CP-10(2)[M]-0 NY DOH SSP v3.1 CP-2b[M]-0 PMI DSP Framework RC-1 TJC IM.01.01.03, EP 2 TJC IM.01.01.03, EP 4

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	

Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CMMC Level 3 Subject to CRR V2016 Subject to HITRUST De-ID Framework Requirements Subject to IRS Pub 1075 Compliance Subject to Joint Commission Accreditation Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline
Level 2 Implementation:	Level 1 plus: The business continuity planning process includes the following: 1. identification and agreement of all responsibilities and business continuity procedures; 2. identification of the acceptable loss of information and services; 3. operational procedures to follow pending completion of response, recovery and restoration including: i. alternative storage and processing site possibilities, and ii. emergency power and back-up telecommunications to the primary site; and 4. appropriate education of staff in the agreed procedures and processes, including crisis management. Business continuity plans address organizational vulnerabilities and therefore may contain covered information that needs to be appropriately protected. Copies of business continuity plans are stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site. Management ensures copies of the business continuity plans are up to date and protected with the same level of physical and logical security as applied at the main site. Other material necessary to execute the continuity plans is also stored at the remote location. The organization identifies alternative temporary locations for processing. The necessary third-party service agreements are established to allow for the transfer and resumption of information systems operations of critical business functions within a time-period (e.g., priority of service provisions) as defined by a risk assessment (see 12.b). The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions. The alternate location is at a sufficient distance to escape any damage from a disaster at the main site. The type of configuration for the alternate site is defined by the risk assessment (see 12.b). Acceptable solutions include: 1. cold sites - a facility with adequate space and infrastructure to support the system; 2. warm sites - partially equipped office spaces that contain some or all of the system hardware, software, telecommunications and power sources; 3. hot sites - office spaces configured with all of the necessary system hardware, supporting infrastructure and personnel; and/or 4. mobile sites - self-contained, transportable shells custom-fitted with IT and telecommunications equipment necessary to meet the system requirements. The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions. The organization develops alternate processing site agreements that contain Priority-of-Service provisions in accordance with the organization's availability requirements, including recovery time objectives (RTOs). The organization ensures that

	the alternate processing site provides information security measures equivalent to that of the primary site.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) AICPA 2017 A1.2 CMMC v1.0 PE.3.136-2 CMSRs v3.1 CP-06 (HIGH; MOD) CMSRs v3.1 CP-06(01) (HIGH; MOD) CMSRs v3.1 CP-06(02) (HIGH) CMSRs v3.1 CP-07 (HIGH; MOD) CMSRs v3.1 CP-07(01) (HIGH; MOD) CMSRs v3.1 CP-07(03) (HIGH; MOD) CMSRs v3.1 CP-09 (HIGH; MOD) CMSRs v3.1 CP-09(02) (HIGH) CRR v2016 SCM:G1.Q6 CRR v2016 SCM:MIL3.Q2 De-ID Framework v1 Physical and Environmental Security: General FedRAMP CP-6 FedRAMP CP-6(1) FedRAMP CP-7 FedRAMP CP-7(1) FedRAMP CP-7(3) FFIEC IS v2016 A.6.35(b) IRS Pub 1075 v2016 9.3.6.5 IRS Pub 1075 v2016 9.3.6.6 ISO/IEC 27002:2013 17.1.2 ISO/IEC 27799:2016 11.2.2 ISO/IEC 27799:2016 17.1.2 MARS-E v2 CP-6 MARS-E v2 CP-6(1) MARS-E v2 CP-7 MARS-E v2 CP-7(1) MARS-E v2 CP-7(3) MARS-E v2 CP-7(5) NIST Cybersecurity Framework v1.1 ID.AM-5 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 ID.BE-4 NIST Cybersecurity Framework v1.1 ID.BE-5 NIST Cybersecurity Framework v1.1 PR.AT-1 NIST Cybersecurity Framework v1.1 PR.DS-1 NIST Cybersecurity Framework v1.1 PR.DS-4 NIST Cybersecurity Framework v1.1 PR.IP-9 NIST Cybersecurity Framework v1.1 RS.CO-1 NIST SP 800-53 R4 CP-6(1)[HM]{0} NIST SP 800-53 R4 CP-6[HM]{0} NIST SP 800-53 R4 CP-7(1)[HM]{0} NIST SP 800-53 R4 CP-7(3)[HM]{0} NIST SP 800-53 R4 CP-7(4)[H]{0} NIST SP 800-53 R4 CP-7[HM]{0} NIST SP 800-53 R4 CP-9(6)[S]{0} NIST SP 800-53 R4 SC-36[S]{0} NY DOH SSP v3.1 CP-6(1)[M]-0 NY DOH SSP v3.1 CP-6b[M]-0 NY DOH SSP v3.1 CP-7(1)[M]-0 NY DOH SSP v3.1 CP-7(3)[M]-0 NY DOH SSP v3.1 CP-7c[M]-0 NY DOH SSP v3.1 CP-9(6)[MN]-1 TJC IM.01.01.03, EP 1 TJC IM.01.01.03, EP 2 TJC IM.01.01.03, EP 3

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Bed: Greater than 750 Beds Health Plan/Insurance/PBM: Greater than 7.5 Million Lives HIE Transactions: More than 6 Million Transactions Hospital Admissions: More than 20k Patients IT Service Provider: More than 60 Terabytes(TB) Non-IT Service Provider: More than 100 Megabytes(MB) Pharmacy Companies: Greater than 60 million Prescriptions Physician Count: Greater than 25 Physicians

	Physician Encounters: Greater than 180k Encounters Record Count Annual: More than 725k Records Record Total: More than 60 Million Records
Level 3 System Factors:	
Level 3 Regulatory Factors:	Subject to FedRAMP Certification Subject to FISMA Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NIST SP 800-53 R4 (Supplemental) Subject to NY OHIP Moderate-Plus Security Baseline Subject to the CMS Minimum Security Requirements (High)
Level 3 Implementation:	Level 2 plus: The organization establishes alternate telecommunications services, including necessary agreements to permit the resumption of information system operations for essential missions and business functions within business defined time period, when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. The organization: 1. Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and 2. Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier. The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery of the information system after a failure or other contingency is done in a trusted, secure, and verifiable manner. Secure information system recovery and reconstitution include, but is not limited to: 1. resetting all system parameters (either default or organization-established); 2. reinstalling patches; 3. reestablishing configuration settings; 4. reinstalling application and system software; and 5. fully testing the system.
Level 3 Control Standard Mapping:	CMSRs v3.1 CP-08 (HIGH; MOD) CMSRs v3.1 CP-08(01) (HIGH; MOD) CMSRs v3.1 CP-08(02) (HIGH; MOD) CMSRs v3.1 CP-08(03) (HIGH; MOD) CMSRs v3.1 CP-08(04) (HIGH) FedRAMP CP-8(1) FedRAMP CP-8(2) ISO/IEC 27002:2013 17.1.2 ISO/IEC 27799:2016 17.1.2 MARS-E v2 CP-8 MARS-E v2 CP-8(1) MARS-E v2 CP-8(2) NIST Cybersecurity Framework v1.1 ID.AM-5 NIST Cybersecurity Framework v1.1 ID.BE-5 NIST SP 800-53 R4 CP-11[S]{0} NIST SP 800-53 R4 CP-2(1)[HM]{0} NIST SP 800-53 R4 CP-2a[HML]{1} NIST SP 800-53 R4 CP-8(1)[HM]{0}

	NIST SP 800-53 R4 PE-17c[HM]{1} NIST SP 800-53 R4 SC-24[H]{0} NY DOH SSP v3.1 CP-8(1)a[M]-0 NY DOH SSP v3.1 CP-8(1)b[M]-0 NY DOH SSP v3.1 CP-8(2)[M]-0

Level CMS	Implementation Requirements
Level CMS Implementation:	The business continuity plan: 1. identifies essential CMS missions and business functions and associated contingency requirements; 2. addresses maintaining essential CMS missions and business functions despite an information system disruption, compromise, or failure. The organization plans for the resumption of essential missions and business functions within the approved Maximum Tolerable Downtime (MTD) for the business functions. Ensure all equipment and supplies required for resuming system operations at the alternate processing site are available, or contracts are in place to support delivery to the site, to permit resumption of system Recovery Time Objectives (RTOs) and business function Maximum Tolerable Downtimes (MTDs). Ensure alternate telecommunications Service Level Agreements (SLAs) are in place to permit resumption of system Recovery Time Objectives (RTOs) and business function Maximum Tolerable Downtimes (MTDs). The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential CMS missions and business functions. The organization provides the capability to reimage information system components and support target recovery times from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components. The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations. The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives. The organization plans for the continuance of Primary Mission Essential Functions (PMEFs) with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites. The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing (see 12.e, Level 2). Alternate telecommunications service providers that are sufficiently separated from the organizations primary service provider are identified, and agreements are established, to ensure these service providers are not susceptible to the same hazards. The organization: 1. Requires primary and alternate telecommunications service providers to have contingency plans; 2. Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and 3. Obtains evidence of contingency testing/training by providers within every 365 days.

	The organization plans for the resumption of all missions and business functions within the approved Maximum Tolerable Downtime (MTD) for the business functions.

Level EHNAC Implementation Requirements	
Level EHNAC Implementation:	The business continuity plans provide assurance that all critical services will be operational with a defined RPO (Recovery Point Objective) that does not exceed 48 hours, and a defined RTO (Recovery Time Objective) that does not exceed 48 hours.

Level FedRAMP Implementation Requirements	
Level FedRAMP Implementation:	The service provider defines a time period consistent with the recovery time objectives and business impact analysis for alternative processing sites. The organization ensures alternate telecommunications Service Level Agreements (SLAs) are in place with the service provider to permit the resumption of information system operations for essential missions and business functions within Recovery Time Objectives and business impact analysis when primary telecommunications capabilities are unavailable. The service provider ensures that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system.

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation:	The agency must identify alternative storage sites and initiate necessary agreements to permit the secure storage of information system and FTI backups and ensure the alternative storage sites provide information security safeguards that meet the minimum FTI protection and disclosure provisions of IRS 6103.

Level HIX Implementation Requirements	
Level HIX Implementation:	Ensure all equipment and supplies required for resuming system operations at the alternate processing site are available, or contracts are in place to support delivery to the site, to permit resumption of essential missions and business functions within one week of contingency plan activation. The organization ensures alternate telecommunications Service Level Agreements (SLAs) are in place to permit resumption of information system operations for essential missions and business functions within a system owner defined, business owner approved time period consistent with the Recovery Time Objectives, Maximum Tolerable Downtimes (MTDs) and business impact analysis for the system when primary telecommunications capabilities are unavailable.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation:	The organization maintains the contact information for individuals with incident handling responsibilities in the system Incident Response Plan and documents changes in the system Incident Response Plan within three [3] days of the change. The organization identifies incidents and responses to classes of incident to ensure continuation of organizational missions and business functions. Classes of incident are

based on attack vector (e.g., attack via external media, the web, improper system use, loss of equipment) and serve to further define specific handling procedures.

The organization identifies emergencies, vandalism, security incidents, or natural disasters and reasonable and appropriate policies and procedures consistent with federal laws and regulations and organizational requirements to ensure continuation of organizational missions and business functions.

The organization creates written guidelines for prioritizing incidents.

The organization develops a contingency plan for the information system in accordance with NIST SP 800-34 that (i) identifies essential CMS missions and business functions and associated contingency requirements, (ii) provides recovery objectives, restoration priorities, and metrics, (iii) addresses contingency roles and responsibilities, and assigns these to specific individuals with contact information; (iv) addresses maintaining essential CMS missions and business functions despite an information system disruption, compromise, or failure; (v) addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and (vi) is reviewed and approved by designated officials within the organization.

The organization communicates contingency plan changes to key contingency personnel, system administrator, database administrator, and other personnel/roles as appropriate and defined organizational elements.

The organization protects the contingency plan from unauthorized disclosure and modification.

The organization continuously monitors and assesses the system to ensure that it is operating as intended and that changes do not have an adverse effect on system performance.

The organization verifies that the provisioned implementation being assessed and/or monitored meets users' needs and is an approved system configuration.

Organizations require a suite of plans to prepare themselves for response, continuity, recovery, and resumption of mission/business processes and information systems in the event of a disruption. Each plan has a specific purpose and scope: (i) Continuity of Operations Plan (COOP), (ii) Business Continuity Plan (BCP), (iii) Critical Infrastructure Protection (CIP) Plan, (iv) Disaster Recovery Plan (DRP), (v) Information System Contingency Plan (ISCP), (vi) Cyber Incident Response Plan, and (vii) Occupant Emergency Plan (OEP).

The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery of the information system after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.

The organization ensures secure information system recovery and reconstitution includes but is not limited to: the (i) resetting of all system parameters (either default or organization-established), (ii) reinstalling patches, (iii) reestablishing configuration settings, (iv) reinstalling application and system software, and (v) fully testing the system.

Control Reference: 2.d Business Continuity Planning Framework

Control Specification:	A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance. *Required for HITRUST Certification CSF v9.6
Factor Type:	Organizational
Topics:	Contingency Planning; IT Organization and Management Roles and Responsibilities; Maintenance; Policies and Procedures; Services and Acquisitions

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CMMC Level 5 Subject to FISMA Compliance Subject to IRS Pub 1075 Compliance Subject to Joint Commission Accreditation Subject to MARS-E Requirements Subject to Texas Health and Safety Code Subject to the CMS Minimum Security Requirements (High)
Level 1 Implementation:	The organization creates, at a minimum, one business continuity plan. The business continuity plan describes the approach for continuity ensuring, at a minimum, and the approach to maintain information or information asset availability and security. The plan also specifies the escalation plan and the conditions for its activation, as well as the individuals responsible for executing each component of the plan. When new requirements are identified, any existing emergency procedures (e.g., evacuation plans or fallback arrangements) are amended as appropriate. The plan has a specific owner. Emergency procedures, manual "fallback" procedures, and resumption plans are within the responsibility of the owner of the business resources or processes involved. Fallback arrangements for alternative technical services, such as information processing and communications facilities, are usually the responsibility of the service providers. The business continuity planning framework addresses the identified information security requirements, including the following: 1. the conditions for activating the plans which describe the process to be followed (e.g., how to assess the situation, who is to be involved) before each plan is activated; 2. emergency procedures which describe the actions to be taken following an incident that jeopardizes business operations; 3. fallback procedures which describe the actions to be taken to move essential business activities or support services to alternative temporary locations, and to bring business processes back into operation in the required time scales; 4. resumption procedures which describe the actions to be taken to return to normal business operations; 5. a maintenance schedule which specifies how and when the plan will be tested, and the process for maintaining the plan; 6. awareness, education, and training activities which are designed to create understanding of the business continuity processes and ensure that the processes continue to be effective; and 7. the critical assets and resources needed to be able to perform the emergency, fallback and resumption procedures.

Level 1 Control Standard Mapping:	1 TAC § 390.2(a)(1) 1 TAC § 390.2(a)(4)(A)(xi) CAQH Core Phase 1 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.4 CAQH Core Phase 2 202: Certification Policy v2.1.0 Subsection 3.4 CMMC v1.0 RE.5.140-2 CMSRs v3.1 CP-02 (HIGH; MOD) CRR v2016 SCM:G1.Q3 CRR v2016 SCM:G3.Q2 CRR v2016 SCM:G4.Q1 CSA CCM v3.0.1 BCR-01 FedRAMP CP-2 FFIEC IS v2016 A.6.35(a) FFIEC IS v2016 A.6.35(c) IRS Pub 1075 v2016 9.3.6.2 ISO/IEC 27002:2013 17.1.2 ISO/IEC 27799:2016 17.1.2 MARS-E v2 CP-2 NIST Cybersecurity Framework v1.1 DE.AE-5 NIST Cybersecurity Framework v1.1 ID.AM-5 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 ID.BE-5 NIST Cybersecurity Framework v1.1 PR.AT-1 NIST Cybersecurity Framework v1.1 PR.IP-7 NIST Cybersecurity Framework v1.1 PR.IP-9 NIST Cybersecurity Framework v1.1 RS.CO-1 TJC IM.01.01.03, EP 1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to CRR V2016 Subject to Supplemental Requirements
Level 2 Implementation:	Level 1 plus: Each business unit creates, at a minimum, one business continuity plan. Procedures are included within the organization's change management program to ensure that business continuity matters are always addressed and timely as part of the change management process. A business continuity planning framework addresses the identified information security requirements and the following: 1. temporary operational procedures to follow pending completion of recovery and restoration; and 2. the responsibilities of the individuals, describing who is responsible for executing which component of the plan. Alternatives are nominated as required.
Level 2 Control Standard Mapping:	CRR v2016 SCM:G1.Q3 ISO/IEC 27002:2013 17.1.2 ISO/IEC 27799:2016 17.1.2 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 PR.AT-1 NIST Cybersecurity Framework v1.1 PR.IP-9

	NIST Cybersecurity Framework v1.1 RS.CO-1 SR v6.4 15a-1

Control Reference: 12.e Testing, Maintaining and Re-Assessing Business Continuity Plans

Control Specification:	Business continuity plans shall be tested and updated regularly, at a minimum annually, to ensure that they are up to date and effective.
Factor Type:	Organizational
Topics:	Awareness and Training; Contingency Planning; IT Organization and Management Roles and Responsibilities; Personnel

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to Joint Commission Accreditation Subject to NY OHIP Moderate-Plus Security Baseline Subject to Texas Health and Safety Code
Level 1 Implementation:	Business continuity plan tests ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security and know their role when a plan is invoked. The test schedule for business continuity plan(s) indicates how and when each element of the plan is tested. These techniques are applied on a 'programmatic' basis such that the tests build upon one another, and in a way that is relevant to the specific response and recovery plan. The results of tests are recorded, and actions taken to improve the plans, where necessary. Updates will also consider lessons learned from implementation of the business continuity plan(s). Responsibility is assigned for regular reviews of at least a part of the business continuity plan, at a minimum, annually. The identification of changes in business arrangements not yet reflected in the business continuity plan is followed by an update of the plan. Changes where updating of business continuity plans are made are acquisition of new equipment, upgrading of systems and changes in: 1. personnel; 2. location, facilities, and resources; 3. legislation; 4. processes, or new or withdrawn ones; and 5. risk (operational and financial).
Level 1 Control Standard Mapping:	AICPA 2017 A1.3 CMSRs v3.1 CP-02 (HIGH; MOD) CMSRs v3.1 CP-04 (HIGH; MOD) CRR v2016 SCM:G1.Q3 CRR v2016 SCM:G2.Q1 CRR v2016 SCM:G3.Q2 CRR v2016 SCM:G3.Q3 CRR v2016 SCM:G3.Q4 CRR v2016 SCM:G3.Q5 CRR v2016 SCM:G4.Q2 CRR v2016 SCM:G4.Q3 CRR v2016 SCM:MIL3.Q2 CRR v2016 SCM:MIL4.Q1 CRR v2016 SCM:MIL5.Q2 CSA CCM v3.0.1 BCR-02 FedRAMP CP-2

	FedRAMP CP-4 ISO/IEC 27002:2013 17.1.3 ISO/IEC 27799:2016 17.1.3 MARS-E v2 CP-2 MARS-E v2 CP-4 NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 ID.SC-5 NIST Cybersecurity Framework v1.1 PR.IP-10 NIST Cybersecurity Framework v1.1 PR.IP-7 NIST Cybersecurity Framework v1.1 PR.IP-9 NIST Cybersecurity Framework v1.1 RC.IM-1 NIST Cybersecurity Framework v1.1 RC.IM-2 NIST Cybersecurity Framework v1.1 RS.CO-1 NY DOH SSP v3.1 CP-2e[M]-2 PMI DSP Framework RC-3 TJC IM.01.01.03, EP 5

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to Banking Requirements Subject to CRR V2016 Subject to EHNAC Accreditation Subject to FedRAMP Certification Subject to FISMA Compliance Subject to HIPAA Security Rule Subject to IRS Pub 1075 Compliance Subject to MARS-E Requirements Subject to NIST SP 800-53 R4 (High) Subject to NIST SP 800-53 R4 (Low) Subject to NIST SP 800-53 R4 (Moderate) Subject to NY OHIP Moderate-Plus Security Baseline
Level 2 Implementation:	Level 1 plus: Each element of the plan(s) is tested at least annually. A variety of techniques is used in order to provide assurance that the plan(s) will operate in real life including: 1. table-top testing of various scenarios (discussing the business recovery arrangements using example interruptions); 2. simulations (particularly for training people in their post-incident/crisis management roles); 3. technical recovery testing (ensuring information systems can be restored effectively) including: i. system parameters are set to secure values; ii. security critical patches are reinstalled; iii. security configuration settings are reset; iv. system documentation and operating procedures are readily available;

	v. application system software is reinstalled and configured with secure settings; and vi. information from the most recent secure back-up(s) is loaded; 4. testing recovery at an alternate site (running business processes in parallel with recovery operations away from the main site); 5. tests of supplier facilities and services (ensuring externally provided services and products will meet the contracted commitment); and 6. complete rehearsals (testing that the organization, personnel, equipment, facilities, and processes can cope with interruptions). The organization reviews test results and initiates corrective actions to ensure the continued effectiveness of the plan. Responsibility is assigned for regular formal reviews of each business continuity plan, which ensures that the updated plans are distributed and reinforced by yearly reviews of the complete plan. The organization coordinates business continuity plan testing and/or exercises with organizational elements responsible for related plans.
Level 2 Control Standard Mapping:	1 TAC § 390.2(a)(4)(A)(xi) 45 CFR Part § 164.308(a)(7)(ii)(D) HIPAA.SR-1 45 CFR Part § 164.308(a)(7)(ii)(D) HIPAA.SR-2 CMSRs v3.1 CP-02 (HIGH; MOD) CMSRs v3.1 CP-04 (HIGH; MOD) CMSRs v3.1 CP-04(01) (HIGH; MOD) CMSRs v3.1 CP-04(02) (HIGH) CRR v2016 SCM:G2.Q1 CRR v2016 SCM:G3.Q4 CRR v2016 SCM:MIL3.Q2 CRR v2016 SCM:MIL4.Q1 FedRAMP CP-2 FedRAMP CP-4 FedRAMP CP-4(1) FFIEC IS v2016 A.6.35(c) IRS Pub 1075 v2016 9.3.6.2 IRS Pub 1075 v2016 9.3.6.4 ISO/IEC 27002:2013 17.1.3 ISO/IEC 27799:2016 17.1.3 MARS-E v2 CP-2 MARS-E v2 CP-4 MARS-E v2 CP-4(1) NIST Cybersecurity Framework v1.1 ID.AM-6 NIST Cybersecurity Framework v1.1 ID.GV-3 NIST Cybersecurity Framework v1.1 ID.SC-5 NIST Cybersecurity Framework v1.1 PR.IP-10 NIST Cybersecurity Framework v1.1 PR.IP-7 NIST Cybersecurity Framework v1.1 PR.IP-9 NIST Cybersecurity Framework v1.1 RC.IM-1 NIST Cybersecurity Framework v1.1 RC.IM-2 NIST Cybersecurity Framework v1.1 RS.CO-1 NIST SP 800-53 R4 CP-2a[HML]{6} NIST SP 800-53 R4 CP-2d[HML]{0} NIST SP 800-53 R4 CP-2e[HML]{0} NIST SP 800-53 R4 CP-4(1)[HML]{0} NY DOH SSP v3.1 CP-2(1)[M]-0 NY DOH SSP v3.1 CP-2d[M]-0 NY DOH SSP v3.1 CP-2e[M]-1 NY DOH SSP v3.1 CP-3(1)[HN]-2 NY DOH SSP v3.1 CP-4(1)[M]-0 TJC IM.01.01.03, EP 5

Level CMS Implementation Requirements

Level CMS Implementation:	The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.

Level FTI Custodians Implementation Requirements	
Level FTI Custodians Implementation:	Both incremental and special purpose data backup procedures are required, combined with off-site storage protections and regular test-status restoration, to validate disaster recovery and business process continuity. Standards and guidelines for these processes are bound by agency policy and are tested and verified.

Level NYDOH Implementation Requirements	
Level NYDOH Implementation:	The organization tests the incident response capability for the information system within every 365 days using NIST SP 800-61, reviews, analyses, and simulations to determine the incident response effectiveness and documents the results. The organization (i) tests incident response capability using (a) checklists, (b) walk-through, discussion-based exercises, or tabletop exercises, (c) comprehensive, functional exercises executed in a simulated operational environment, and (d) automated mechanisms, as applicable. (ii) Documents results for assessment and potential process improvement. The organization coordinates incident response testing with organizational elements responsible for related plans. The organization (i) tests the contingency plan for the information system within every 365 days using NIST (NIST SP 800-34, NIST SP 800-84) and CMS-defined tests and exercises, such as tabletop tests, in accordance with the current CMS contingency plan procedure to determine the effectiveness of the plan and the organizational readiness to execute the plan; (ii) reviews the contingency plan test results; and (iii) initiates corrective actions, if needed. The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.

Control Category: 13.0 - Privacy Practices

Objective Name: 13.01 Transparency

Control Objective:	Policies, procedures, and technologies that directly affect data subjects and/or their PII are open and transparent.

Control Reference: 13.a Privacy Notice

Control Specification:	Data Subjects have a right to adequate and easily accessible notice of the use and disclosures of their PII that may be made by the PII controller, and of the data subject's rights and the controller's legal duties with respect to PII.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Privacy)
Level 1 Implementation:	Organizations will provide a plain-language privacy notice to data subjects outlining their practices and policies regarding PII, in a manner and timeframe required by applicable law and/or regulation and in a manner that can be understood by individuals not familiar with information technologies, legal jargon and the Internet. Organizations will revise their notices to reflect any changes in their practices, policies or activities that affect PII, before or as soon as practicable after the change. All reasonable and practical steps will be taken to ensure that such notice is provided to data subjects before or at the time of collection of PII or as soon as is practical.
Level 1 Control Standard Mapping:	45 CFR Part § 164.520(a) HIPAA.PR AICPA 2017 CC2.2 AICPA 2017 P1.1 APEC II 15 APEC II 16 CMSRs v3.1 TR-01 (HIGH; MOD) CMSRs v3.1 TR-03 (HIGH; MOD) EU GDPR Article 13(1) EU GDPR Article 14(1) ISO/IEC 29100:2011 5.8 ISO/IEC 29151:2017 A.9.1(c) ISO/IEC 29151:2017 A.9.1(e) ISO/IEC 29151:2017 A.9.1(f) MARS-E v2 TR-1 MARS-E v2 TR-1(1) MARS-E v2 TR-3 NIST SP 800-53 R4 IP-1[P]{0} NIST SP 800-53 R4 TR-1[P]{0}

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Privacy)
Level 2 Implementation:	When statutory language is written broadly, organizations ensure there is a close nexus between the general authorization and any specific collection of PII by clearly describing the purposes in related privacy compliance documentation. The organization provides real-time and/or layered notice when it collects PII. The organization (i) publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII); (ii) keeps SORNs current; (iii) includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected; and (iv) publishes SORNs on its public website.
Level 2 Control Standard Mapping:	CMSRs v3.1 AP-02 (HIGH; MOD) CMSRs v3.1 TR-01(01) (HIGH; MOD) CMSRs v3.1 TR-02 (HIGH; MOD) CMSRs v3.1 TR-02(01) (HIGH; MOD) MARS-E v2 TR-2 MARS-E v2 TR-2(1) NIST SP 800-53 R4 TR-1(1)[P]{0} NIST SP 800-53 R4 TR-2(1)[P]{0} NIST SP 800-53 R4 TR-2[P]{0}

Level EHNAC Implementation Requirements

Level EHNAC Implementation:	The organization ensures it satisfies the implementation specifications listed in the HIPAA Privacy Rule for individual rights.

Level GDPR Implementation Requirements

Level GDPR Implementation:	Notices to data subjects regarding their rights must be provided in an easily accessible and easily understood form available in writing or electronically. Particular care in ensuring the language is clear and plain is taken if the notice will be used with children. The notice can be provided orally upon the request of the data subject. The notice will be provided to the data subject within a reasonable time given the type of data and use thereof; this must be within a month of the data collection. If the data is used to contact the data subject, the notice will be given when the data subject is contacted. If the data is being shared, the notice will be provided before the sharing occurs. An additional or new notice must be provided to the data subject before using the data for a different purpose than that of the original collection.

	The notice does not need to be given if: the data subject already has the information; it would be impossible or overly burdensome to provide it; the collection is done in conjunction with an EU or Member State law that provides protection for the data subject; or if it must remain confidential due to an EU or Member State law. Notices may be impractical if the data is collected for archival in the public interest, scientific or historical research, or statistical purposes. In those cases, the age of the data and safeguards adopted is considered. Privacy notice information and responses relating to a data subject's request to exercise his/her rights must be provided free of charge, unless the data subject's requests are excessive and/or repetitive. In such cases, a reasonable fee may be charged, or the controller can refuse to act on the request.

Level Group Health Plans	Implementation Requirements
Level Group Health Plans Implementation:	The health insurance issuer or HMO provides an individual, other than an inmate enrolled in a group health plan, a notice of privacy practices for that portion of the group health plan through which the individual receives benefits; provides such notice to the named insured of a policy under which coverage is provided to the named insured and one or more dependents; and gives such notice to new enrollees at the time of enrollment and again within 60 days of any material revision to the notice. At a minimum of once every three years, the health plan notifies individuals then covered by the plan, of the availability of the notice and how to obtain the notice.

Level HIPAA	Implementation Requirements
Level HIPAA Implementation:	If the covered entity provides a health plan, the covered entity provides notice or notices relevant to the individual (other than an inmate) no later than the compliance date or upon enrollment thereafter, within 60 days of a material revision, and no less than every three years. A covered entity may provide the notice of privacy practices to an individual by email, if the individual agrees to electronic notice, and the agreement has not been withdrawn.

Level Texas Covered Entities	Implementation Requirements
Level Texas Covered Entities Implementation:	The hospital maintains a patient's right to personal privacy and the confidentiality of personal information and clinical records. Nursing and other facilities in which a patient is resident maintain a patient's right to personal privacy and the confidentiality of personal information and clinical records. A patient's right to personal privacy and the confidentiality of personal information and clinical records is maintained at intermediate care facilities such as those for persons with an intellectual disability or related conditions. Ambulatory surgical centers maintain a patient's right to personal privacy and the confidentiality of personal information and clinical records. Outpatient facilities such as those for end-stage renal disease maintain a patient's right to personal privacy and the confidentiality of personal information and clinical records. Special care facilities such as those for AIDS patients maintain a patient's right to personal privacy and the confidentiality of personal information and clinical records.

	Psychiatric (mental) facilities maintain a patient's right to personal privacy and the confidentiality of personal information and clinical records. Parents of a minor child retain the rights and duties specified by law. Parents, foster parents, guardians, or managing conservators of a minor child with special healthcare needs or adult clients with special needs retain the rights and duties specified by law.

Control Reference: 13.b Openness and Transparency

Control Specification:	To provide data subjects with clear and easily accessible information about the PII controller’s policies, procedures and practices with respect to the handling of PII.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CCPA Requirements Subject to NIST SP 800-53 R4 (Privacy) Subject to the EU GDPR
Level 1 Implementation:	Provide data subjects with clear and easily accessible information about the organization's policies, procedures and practices with respect to the processing of PII. Organizations will disclose the choices and means which are offered by the organization to data subjects for the purposes of limiting the processing of, and for accessing, correcting and removing their PII. Organizations will ensure they provide effective notice to data subjects regarding: 1. Its activities that impact privacy including, but not limited to, the collection, use, sharing, safeguarding, maintenance, and disposal of PII; 2. Authority for collecting PII; 3. The PII collected, the purpose(s) for which it is collected and how it will be protected; 4. The choice, if any, data subject may have regarding how the PII controller uses PII and the consequence of exercising or not exercising those choices; 5. The ability to object to the processing; 6. If the PII controller intends to levy any fees for access, as may be permitted by law in some jurisdictions; 7. How long the PII will be retained; 8. How data subjects may obtain access to their PII for the purpose of amendment or correction, where appropriate; 9. Whether the PII controller shares PII with external entities and the purposes for such sharing; 10. Whether the organization on-sells or forwards the data for processing by data analytics organizations and the details applicable to PII risks; and 11. How data subjects are able to communicate with the organization's privacy officials to provide feedback, including but not limited to complaints and/or direct questions regarding privacy practices.

Level 1 Control Standard Mapping:	AICPA 2017 P1.1 AICPA 2017 P2.1 AICPA 2017 P6.7 AICPA 2017 P8.1 APEC II 15 APEC II 15(a) APEC II 15(b) APEC II 15(c) APEC II 15(d) APEC II 15(e) APEC II 16 CCPA 1798.100(b) CCPA 1798.110(a) EU GDPR Article 13(1) EU GDPR Article 13(1)(a) EU GDPR Article 13(1)(c) EU GDPR Article 14(1) ISO/IEC 29100:2011 5.8 ISO/IEC 29151:2017 A.10.1(n) ISO/IEC 29151:2017 A.9.1(a) ISO/IEC 29151:2017 A.9.1(a)(1) ISO/IEC 29151:2017 A.9.1(a)(2) ISO/IEC 29151:2017 A.9.1(a)(3) ISO/IEC 29151:2017 A.9.2 ISO/IEC 29151:2017 A.9.2(a) ISO/IEC 29151:2017 A.9.2(b) ISO/IEC 29151:2017 A.9.2(c) ISO/IEC 29151:2017 A.9.2(e) ISO/IEC 29151:2017 A.9.2(f) ISO/IEC 29151:2017 A.9.2(g) ISO/IEC 29151:2017 A.9.2(h) ISO/IEC 29151:2017 A.9.2(i) ISO/IEC 29151:2017(a)(4) NIST SP 800-53 R4 TR-3b[P]{0} NIST SP 800-53 R4 UL-2a[P]{0} PDPA 11(5) PDPA 20(1)(e)

Level CCPA Implementation Requirements

Level CCPA Implementation:	Businesses are required to notify consumers of their right to request deletion. Businesses that sell information or disclose it for a business purpose are required to disclose in their notice to consumers the categories of personal information it has sold and/or disclosed for a business purpose or that it has not sold and/or disclosed any. Businesses that sell information to third-parties are required to disclose in their notice to consumers that they have the right to opt-out. Before offering financial incentives to consumers, businesses are required to provide notice of the incentives, receive the consumer's opt-in to the program, and not use incentives that are unjust or unreasonable. Businesses are required to: 1. Provide notices to consumers in a reasonably accessible form that includes information on how to submit requests for information. Businesses must provide a toll-free number to request information unless all business is conducted online and a web address to do so if the business maintains a website. 2. Respond to consumer requests within 45 days of receipt, which may be extended an additional 45 days if reasonably necessary. The time period to respond to a consumer request may be extended by an additional 90 days if the requests are complex or numerous so long as the consumer is notified of the delay within 45 days of receiving the request. Disclosures should cover the 12-month period prior to the request. If the business decides not to honor a consumer request, it must tell the consumer without delay, informing the consumer why their request was not honored and notifying them of any appeal

	processes. Businesses may charge a reasonable fee based on related administrative costs for excessive or unfounded requests, but they must be able to show the requests are excessive or unfounded. 3. Provide access promptly and free of charge through the consumer's account or by mail or electronically in a readily useable format that allows for data portability. If the business has an online privacy notice, it is required to include: 1. A description of the consumer rights under 1798.110, 115, and 125, and one or more designated methods for submitting requests; 2. A list of categories of information it has collected about consumers in the preceding 12-month period, as outlined in 1798.110(c); and 3. A list of categories of information it has sold and/or disclosed about the consumers in the preceding 12-month period, as outlined in 1798.115(c); if no information has been sold and/or disclosed for a business purpose during that time period, the business should say so in the notice. Businesses which sell personal information to third-parties are required to provide a reasonably accessible notice to consumers that: 1. Provide a clear and conspicuous link on its website homepage, titled "Do Not Sell My Personal Information", which enables the consumer, or person authorized, to opt-out of the sale of personal information. The business may not require a consumer to open an account to exercise their opt-out right; 2. Include a description of the consumer's rights and a separate link to the "Do Not Sell My Personal Information" webpage in its online privacy notice or in any California-specific privacy notice; 3. Ensure that anyone who handles consumer inquiries knows the relevant requirements; 4. Refrain from selling information of a consumer who has opted-out; 5. Respect the consumer's decision to opt-out for at least 12 months before seeking authorization to selling information again; and 6. Use personal information provided in an opt-out request only for complying with the request.
Level GDPR	**Implementation Requirements**
Level GDPR Implementation:	An adequate privacy notice includes information on data retention and data subject rights as well as available remedies. Adequate notices include contact information for the controller and, if applicable, the data protection officer, the purposes and legal basis for processing, the categories of data concerned, the recipients or types of recipients of the data, and, if applicable, information about transfers outside the EEA. If automated decision-making including profiling will be done, the data subject must be informed of this and the potential consequences of the profiling or of not providing the necessary information.
Level HIPAA	**Implementation Requirements**
Level HIPAA Implementation:	The covered entity provides individuals with an appropriate notice of the potential uses and disclosures of their PHI that contains required elements (e.g., header, descriptions of uses with at least one example, requirements for authorization).
Level Personal Data Protection Act	**Implementation Requirements**
Level Personal Data Protection Act Implementation:	If a controller receives the data from another controller, it must inform the original controller of the purposes for which the data will be used to ensure proper consent has

	been obtained. The controller must notify the data subject if information is to be used in regard to an employment relationship and, if requested, the contact information of someone able to answer any additional questions the data subject has. Telecommunications providers must notify the PDPC of terminated numbers. [PDP DNCR R 2013]. Telecommunications providers must register with the PDPC before submitting its first information on discontinued numbers. The message must include the identification of the person or entity sending the message and contact information for the sender. It is assumed that this information will be valid for at least 30 days from the time of the message.

Control Reference: 13.c Accounting of Disclosures

Control Specification:	To ensure that disclosures of PII, especially to third-parties, are recorded. To ensure the PII processor notifies the PII controller of any legally binding requests for disclosure of PII. Provisions for the use of subcontractors to process PII should be specified in the contract between the PII processor and the PII controller.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Privacy) Subject to the EU GDPR
Level 1 Implementation:	PII controllers will implement measures to ensure that: 1. PII processors consult with applicable PII controllers prior to accepting any legally binding requests for disclosures of PII, unless otherwise prohibited by law; and 2. PII processors accept any contractually agreed requests for PII disclosures, as authorized by the relevant PII controller, unless otherwise prohibited by law. Information disclosed will include that subcontracting is used and the names of relevant subcontractors, but not any business-specific details. The information disclosed will also include the countries in which subcontractors may process data and how subcontractors are obliged to meet or exceed the obligations of the PII processor. Where public disclosure of subcontractor information is assessed to increase security risk beyond acceptable limits, disclosure will be made under a non-disclosure agreement on the request of the PII controller. The PII controller will be made aware that information about subcontractors being used is available. PII may be disclosed during the course of an organization's normal operations. These disclosures and any additional disclosures to third-parties (e.g., lawful investigations, external audits) will be accurately recorded. The accounting of disclosures will be recorded and retained, as applicable by law, and made available to the data subject named in the record upon request. The records will include: 1. The date, nature and purpose of each disclosure.

	2. The source of the disclosure and the source of the authority to make the disclosure.
Level 1 Control Standard Mapping:	AICPA 2017 P6.2 AICPA 2017 P6.7 ISO/IEC 29151:2017 A.7.3(a) ISO/IEC 29151:2017 A.7.3(b) ISO/IEC 29151:2017 A.7.4 ISO/IEC 29151:2017 A.7.5 NIST SP 800-53 R4 AR-8[P]{1} NIST SP 800-53 R4 AR-8[P]{3}

Level HIPAA Implementation Requirements

Level HIPAA Implementation:	The covered entity provides individuals the right to receive an accounting of disclosures of certain PHI made by the covered entity in the six years prior to the date on which the accounting is requested, except for where restricted by law. The covered entity's accounting of disclosures includes, for the six years prior to the request, the date, a name and address of the entity provided the PHI, a description of the PHI disclosed, and the purpose for which the information was disclosed; and, if for research, the name of the research activity, the period of time the PHI was disclosed, the contact information of the research sponsor (name, address and phone number), and a statement that the PHI may or may not have been disclosed for a particular research activity. When requested by the individual, the covered entity provides assistance to the individual in contacting the research sponsor and researcher for an accounting. The covered entity acts upon an individual's request for an accounting no later than 60 days after receipt of the request (with a one-time 30-day extension with proper notice to the requestor), free of charge for the first request within any 12-month period and, if informed in advance, for a reasonable cost-based fee for subsequent requests within the period. The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures upon the request of a health oversight agency or law enforcement official for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifies the time for which such a suspension is required. The Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) periodically consults with managers of organization systems of record to ensure that the required accountings of disclosures of records are being properly maintained and provided to persons named in those records consistent with the dictates of the Privacy Act.

Objective Name: 13.02 Individual Participation

Control Objective:	Data subjects are provided a reasonable opportunity and capability to access and review their PII and to challenge its accuracy and completeness.

Control Reference: 13.d Consent

Control Specification:	To make data subjects active participants in the decision-making process regarding the processing of their PII, except as otherwise limited by legislation and regulations, through the exercise of meaningful, informed and freely given consent.
Factor Type:	Organizational

Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation:	Where feasible and appropriate or where legally required, organizations will provide means for data subjects, or authorized agents, to provide consent before any PII processing begins. Organizations will ensure that consent adheres to all applicable legal requirements and is obtained in an informed and transparent manner. Organizations determine alternate solutions, if necessary, for cases where the practical means chosen are no longer operational, in order to ensure that consent is obtained before any processing begins. Organizations will store a record of consent. Where feasible and appropriate or where legally required, organizations will obtain consent from data subjects prior to any new uses or disclosures of previously collected PII. Organizations will provide a means for data subjects to modify the scope of their consent. Any modification of consent is acted upon in a timely manner and processing is modified or cease, in accordance with the revised consent. Organizations will confirm, as appropriate, the identity of data subjects and/or authorized agents submitting consent to PII processing. The information requested for verification of identity will be kept to the minimum essential for that purpose, will only be retained for as long as required for that purpose and will be securely disposed of when no longer required.
Level 1 Control Standard Mapping:	AICPA 2017 P2.1 ISO/IEC 29151:2017 A.3.1(a) ISO/IEC 29151:2017 A.3.1(b) ISO/IEC 29151:2017 A.3.1(c) ISO/IEC 29151:2017 A.3.1(d) ISO/IEC 29151:2017 A.3.1(e) ISO/IEC 29151:2017 A.3.1(g) ISO/IEC 29151:2017 A.3.1(h) ISO/IEC 29151:2017 A.3.1(j) PDPA 13

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2	

Regulatory Factors:	
Level 2 Implementation:	Organizations will provide examples to illustrate the potential privacy risks of the authorization.
Level 2 Control Standard Mapping:	CMSRs v3.1 IP-01(01) (HIGH; MOD) MARS-E v2 IP-1(1)

Level CCPA Implementation Requirements

Level CCPA Implementation:	Third-parties are required to obtain explicit consumer consent before selling personal information that has been sold to them by a business. Business obtains consent (opt-in) from consumers under 16 before information may be sold. The consent is required from the consumer if the consumer is between 13 and 16, or from the parent or guardian, if the consumer is younger than 13. Businesses that willfully disregard age information shall be considered to know that the consumer has the right to opt-in.

Level GDPR Implementation Requirements

Level GDPR Implementation:	Consent must be freely given, specific, informed, and unambiguous, in a distinct manner if included in a written declaration, and properly documented. The act of giving consent must be an affirmative act and the controller must be able to demonstrate that the data subject has consented appropriately for processing based on consent. The data subject can withdrawal consent at any time and will be notified of this when consenting. Consent is not to be used as a basis for processing if there is a power differential and services are not to be conditional upon consent when PII is not required to deliver the services. Requiring consent to the use of data that is not necessary to the performance of a contract before providing services is not freely given. A child must be 16 years old before s/he can give valid consent, although Member States can lower that age no less than 13. The controller must make reasonable efforts to verify that consent is given by the responsible adult if the child is not old enough to provide consent on his/her own. Decisions made based on automated processing needed to fulfill a contract, authorized by EU or Member State law that provides privacy safeguards or based on explicit consent from the data subject will not be made using sensitive data without the data subject's explicit consent or if needed for the substantial public interest and proper rights balancing and safeguarding has been performed.

Level HIPAA Implementation Requirements

Level HIPAA Implementation:	When required, the organization does not use or disclose PII without a valid authorization. When feasible, appropriate, and in line with organization's policies, the organization does not share information for which an authorization is not needed without providing the patient an opportunity to consent or object to the disclosure. A valid authorization is required for a variety of disclosures, including the use and disclosure of psychotherapy notes or for marketing purposes. When authorization is required, the covered entity ensures the authorizations are valid by including required core elements.

	If the individual's authorization is given in the context of a written declaration which also concerns other matters, the organization ensures requests for authorization are presented in a manner which is clearly distinguishable from the other matters , in an intelligible and easily accessible form, using clear and plain language. The covered entity will not create compound authorizations, except when combining authorizations for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. However, a covered entity may combine authorizations specifically for the use or disclosure of psychotherapy notes. When combining authorizations, the covered entity must ensure there is no condition on the provision of treatment, payments, enrollment in a health plan, or eligibility for benefits for the provision of an authorization except as allowed for research, underwriting and risk determinations, or disclosure of PHI to a third-party, but in no case for the use of psychotherapy notes.

Level Personal Data Protection Act	Implementation Requirements
Level Personal Data Protection Act Implementation:	Data can be collected without consent in certain circumstances. These are delineated in the Second, Third, and Fourth Schedules of the Act. Consent for sending specific messages cannot be required as part of receiving goods or services or based on false or misleading information. Consent may be considered given—or deemed—if a reasonable person would believe the use to be directly related to or required to meet the purpose for which consent was given. Consent may also be implied if the data subject provides the personal data voluntarily to the controller. Consent is given to a second organization if the data subject is deemed to have consented to one organization to send it to the other, such as sending information to a bank in response to a purchase including bank routing or a credit card number.

Level Texas Covered Entities	Implementation Requirements
Level Texas Covered Entities Implementation:	A minor child or a non-parent of a minor child is allowed to consent to treatment for the child by a licensed physician or dentist as specified by law. Nursing or other patient resident facilities ensure residents approve the release of personal and clinical records. Consent for the release of confidential information related to a minor child are written and signed as specified by law.

Control Reference: 13.e Choice

Control Specification:	To present to data subjects, where appropriate and feasible, the choice not to allow the processing of their PII, to refuse or withdraw consent or to oppose a specific type of processing, and to explain to data subjects the implications of granting or refusing consent.
Factor Type:	Organizational
Topics:	

Level 1	Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to EHNAC Accreditation
Level 1 Implementation:	The organizations will ensure that data subjects are provided the opportunity to exercise a choice regarding the processing of their PII and can do so before any processing takes place. Where provided for by relevant legislation or regulation, data subjects, upon giving reasonable notice to the Organization, can withdraw consent at any time. If legal grounds are required to exercise the right to object, organizations will ensure that the data subject exercising their right to object provide reasonable grounds for the objection. If the organization refuses to comply with the objection, detailed reasons for why the organization does not consider those grounds as legitimate will be documented. Where possible and practical, organizations provide data subjects with the ability to object to specific aspects of the PII processing, rather than data subjects having to accept or object to the PII processing in its entirety. Organizations will acknowledge the data subject's statement of objection within the time frame specified in applicable laws or as defined in the organization's policy. Organizations will not withhold services from a data subject who declines to provide PII that is not relevant to that service. Organizations will confirm the identity of the data subject and/or authorized agent, submitting an objection to processing. The information requested for identity verification will be kept to a minimum essential for that purpose, will only be retained for as long as required for that purpose and will be securely disposed of when no longer required. Organizations will ensure that all necessary entities are made aware of any objections submitted by the data subject, and that the entities abide by any valid objections.
Level 1 Control Standard Mapping:	45 CFR Part § 164.530(g) HIPAA.PR AICPA 2017 P2.1 ISO/IEC 29151:2017 A.3.2 ISO/IEC 29151:2017 A.3.2(b) ISO/IEC 29151:2017 A.3.2(d) ISO/IEC 29151:2017 A.3.2(g) ISO/IEC 29151:2017 A.3.2(j) PDPA 16

Level CCPA Implementation Requirements

Level CCPA Implementation:	Businesses ensure that consumers who exercise any of their rights are not discriminated against through pricing or quality of goods or services. Businesses may charge a consumer a different rate if it is reasonably related to the value to the consumer of the consumer’s data.

Level GDPR Implementation Requirements

Level GDPR Implementation:	When first communicating with the data subject, the controller must inform him/her of the rights to object. Data subjects may withdraw consent at any time and are made aware of this right. Withdrawing consent must be as easy as giving it. The right to object does not apply if the data processing is needed to fulfill a contract, is authorized by EU or Member State law that provides privacy safeguards or is based on explicit consent from the data subject. In certain circumstances, the controller must restrict processing of data upon request from the data subject. This includes when: the accuracy of the data is being reviewed or contested; the processing is unlawful, and the data subject wants restrictions instead of

	erasure; the controller no longer needs the data except with respect to legal claims; or the data subject objects to the processing, and a review is occurring as to whether the controller can override the objections. Restrictions can be done by moving the data to another system, making it unavailable to users, or taking it down from a published site. If the data is in an automated filing system, the restriction must be done using technical means that ensure it is not processed and cannot be changed. The system displays information showing the data is under a restriction. Once a restriction is granted, the data will only be processed by storing it, upon the data subject's consent, in relation to a legal claim, for the protection of a legal or natural person, or in the public interest of the EU or a Member State . The controller must notify the data subject before lifting a restriction. The data subject can object at any time to the use of his/her data for direct marketing or related profiling. Upon notification of the objection, the controller must stop the processing of data for direct marketing or related profiling. The data subject may object to online entity using data for automated means using technical tools, including as an example a browser's "do not track" feature. The data subject may object to decisions made based on automated processing that have legal or other significant impacts on the data subject. Based on his or her situation, a data subject may object to processing for scientific, historical, or statistical purposes. If the process is necessary for a public interest task, the controller may continue processing the data despite the objection.

Level HIPAA Implementation Requirements

Level HIPAA Implementation:	Under certain conditions, an organization must permit an individual, or their legally-authorized representative, to request that the organization restrict processing (e.g., uses or disclosures) of the individual's PII (e.g., PHI to carry out treatment, payment, or healthcare operations ; however, covered entities are not required to agree to a restriction). A covered entity that agrees to a restriction on use or disclosure must document the restriction in accordance with HIPAA § 164.530(j). The covered entity agrees to, and complies with, requests by individuals for restrictions on disclosure of PHI to a health plan for a healthcare item or service for which someone other than the health plan pays in full. The covered entity terminates agreements to restrictions if the individual agrees to or requests the termination in writing, an oral agreement is documented, or the covered entity informs the individual, and termination is effective only for PHI created or received thereafter. The covered entity ensures that individuals who exercise any of their lawful rights, including the filing of a complaint, are not subject to intimidation, threats, discrimination, or any other retaliatory action. No later than at the time of the first communication with the individual, the organization informs individuals in advance of an allowed use or disclosure and provides an opportunity to agree to, or prohibit, or restrict the use or disclosure, either orally or in writing, on grounds relating to the subjects particular situation, including processing performed in the public interest, in the exercise of the organizations official authority, or in the legitimate interests of the organization or by a third-party, except where such interests are overridden by the interests or fundamental rights and liberties (freedoms) of the individual which require the protection of PII, particularly for a child.

	If an individual does not object, the covered entity limits the PHI contained in a directory of individuals at its facility to the individual's name, location, general condition, and religious affiliation and only uses or discloses such information for directory purposes to members of the clergy or, except for religious affiliation, to other persons who ask for the individual by name. The covered entity informs individuals of the PHI it may include in a directory, and to whom it may disclose such information, and provides the individual an opportunity to restrict or prohibit some or all of the disclosures. If an individual is present, or has the authority, the covered entity obtains the individual's consent or authorization, provides the individual an opportunity to object, or reasonably infers from the circumstances that the individual does not object to disclosure of PHI. The organization ensures authorizations are freely given and informs individuals they have the right to withdraw the authorization at any time when the request for authorization is made and ensure individuals can withdraw their authorization as easily as it is given.

Level Personal Data Protection Act	Implementation Requirements
Level Personal Data Protection Act Implementation:	People may subscribe to have their numbers on the Do Not Call Register or to have it removed therefrom. Withdraw of consent to specific messages may be done at any time and must be respected.

Control Reference: 13.f Principle Access

Control Specification:	To give data subjects the ability to access and review their PII and to challenge its accuracy and completeness.
Factor Type:	Organizational
Topics:	

Level 1	Implementation Requirements
Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CCPA Requirements Subject to NY OHIP Moderate-Plus Security Baseline
Level 1 Implementation:	The organization will publish a process which governs how data subjects may request access to records maintained in the organization's system. Organizations will allow data subjects to exercise their right of access in order for him/her to assess its accuracy and to request corrections as necessary (where allowed by applicable legislation). Data subjects will be able to exercise their right of access in a timely manner, without undue cost, in a form understandable and accessible to the data subjects and similar to the means used to collect the PII originally (e.g., by regular mail or by email). Responses to the data subjects regarding this will be provided in accordance with applicable legislation, regulation or as specified in the organization's policy. As practical, responses will be provided in a form requested by the data subject.

	Organizations will ensure the data subject's right of access can always be exercised, except where: 1. the burden or expense to PII controllers is unreasonable or disproportionate to the risk of privacy; 2. the PII cannot be disclosed due to legal reasons or the PII is not to be disclosed due to security reasons; or 3. the privacy of persons other than the data subjects would be violated. Organizations will ensure that PII is only accessed by whom the information relates and/or an authorized agent. This may require the authentication of the requesting party's identity. Requirements for such may be defined in applicable legislation or regulation. Where authentication of identification of the PII requestor is required, the organization will determine the appropriate form of identification and authentication, unless otherwise prescribed by regulation. Only the minimum information necessary to verify identification will be requested. This information will be properly secured and only retained for as long as necessary. Before providing a data subject with his/her PII, the organization ensures that all requested information can be provided, while still protecting the rights, freedoms, and PII of other data subjects. Organizations ensure that PII is only sent to authorized parties and in a secure manner. After providing proof of their identity, data subjects expect communication about PII and, if desired, access to PII: 1. within a reasonable time; 2. at a charge, if any, that is not excessive; 3. in a reasonable manner; and 4. in a form that is generally understandable. Organizations will establish and implement a process to notify data subjects submitting requests about the status of their request and the necessary processing (e.g., by postal mail or email, noting that the request has been received and the date by which they can expect to receive a response). When requests are made regarding stored archives, organizations have more flexibility regarding the response time. The organization will inform the data subject submitting the request of the timescale for request processing and provide a reasonable response time. If the organization denies the data subject access to their PII, the organization will provide to the data subject, in a timely manner, reasons why and provide them the opportunity to challenge the denial. PII processors will support the PII controller's facilitation of the exercise of data subject's rights to access, correct or delete their PII.
Level 1 Control Standard Mapping:	45 CFR Part § 164.522(b) HIPAA.PR 45 CFR Part § 164.526(c) HIPAA.PR 45 CFR Part § 164.526(e) HIPAA.PR AICPA 2017 P4.3 AICPA 2017 P5.1 AICPA 2017 P5.2 APEC VIII 23(b) APEC VIII 24 APEC VIII 25 CCPA 1798.100(c) CCPA 1798.105(c) CMSRs v3.1 DI-01 (HIGH; MOD) EU GDPR Article 15(4) EU GDPR Article 16 EU GDPR Article 20(4) ISO/IEC 29100:2011 5.9 ISO/IEC 29151:2017 A.10.1(a) ISO/IEC 29151:2017 A.10.1(c)

	ISO/IEC 29151:2017 A.10.1(d) ISO/IEC 29151:2017 A.10.1(e) ISO/IEC 29151:2017 A.10.1(g) ISO/IEC 29151:2017 A.10.1(h) ISO/IEC 29151:2017 A.10.1(j) ISO/IEC 29151:2017 A.10.1(k) ISO/IEC 29151:2017 A.10.1(l) ISO/IEC 29151:2017 A.10.1(m) ISO/IEC 29151:2017 A.10.1(o) MARS-E v2 DI-1 NY DOH SSP v3.1 AC-3(9).IS.PII1[M]-2 PDPA 21 PDPA 22

Level CCPA Implementation Requirements

Level CCPA Implementation:	The business provides consumers, in response to a verified request, the right to request the categories of personal information collected about them, as well as the actual personal information collected about the consumer. After receiving a verifiable consumer request, the business is required to provide the consumer access to their personal information promptly and free of charge. The personal information must be delivered via the consumer's account, mail, or electronically. If provided electronically the personal information must be portable, and to the extent feasible, in a readily useable format. Businesses are not required to provide access to the personal information more than twice in any 12-month period. Businesses that sell personal information or disclose it for a business purpose provide consumers the right to request. Upon receipt of a verifiable consumer request, the business will disclose the categories of personal information collected about them, the categories of personal information that was sold or disclosed for a business purpose, the categories of third-parties to whom the personal information was sold, and what categories of personal information were sold to which types of third-parties.

Level EHNAC Implementation Requirements

Level EHNAC Implementation:	The organization must determine the level at which PHI is handled, and then respond to all privacy criteria based on that determination. Candidate must identify the level at which PHI is handled based on the following: Level 1: PHI is NEVER directly accessed by any workforce member. Level 2: PHI is sometimes accessible to workforce members. Level 3: PHI is created when workforce members communicate directly with members or patients. Creation of PHI means a designated record check is created. Candidate must ensure that the following Privacy areas are addressed based on the Level determination above. Level 1: • None Level 2: • Review the HIPAA Privacy Rule Uses and Disclosures regulations and document which requirements apply to your business model and the way in which ePHI is handled. Provide evidence of this review along with policy and procedure documents in the respective sections within this self-assessment.

	• Review the HIPAA Privacy Rule Individual Rights regulations and document which requirements apply to your business model and the way in which ePHI is handled. Provide evidence of this review along with policy and procedure documents in the respective sections within this self-assessment. • Provide a general statement as to the determination if it is deemed that NO Uses or Disclosures or Individual Rights are deemed applicable. Level 3: • Review the HIPAA Privacy Rule Uses and Disclosures regulations and document which requirements apply to your business model and the way in which ePHI is handled. Provide evidence of this review along with policy and procedure documents in the respective sections within this self-assessment. • Review the Privacy Rule Individual Rights regulations and document which requirements apply to your business model and the way in which PHI is handled. Provide evidence of this review along with policy and procedure documents in the respective sections within this self-assessment. • Provide a general statement as to the determination if it is deemed that CERTAIN Uses or Disclosures or Individual Rights are deemed applicable.

Level GDPR Implementation Requirements

Level GDPR Implementation:	The data subject has the right to know if the controller has information on him/her and why it is being processed. This information includes the categories and recipients of the personal data, the data retention period, and the data subject's right to complain to the supervisory authority or seek a judicial remedy. If applicable, it also includes where the data came from if not from the data subject and information about automated decision-making if applicable. If a data subject seeks access to information and the controller does not have information sufficient to identify that person, the controller informs the data subject accordingly. The data subject may choose to provide more information to enable data subject rights. The controller is responsible for responding to data subject's request to exercise his/her rights, unless the controller can show it cannot identify the data subject among its information. The controller may ask for more information from the data subject in order to ensure the person asking for information is in fact the subject of the information. The data subject has the right to know what safeguards are in place if the data has been transferred outside the EEA. The data subject has the right to a copy of the personal data the controller has. It will be provided electronically, unless the data subject requests otherwise, and for free, unless the request is duplicative. If the data comes from the data subject and the subject requests, the controller must provide the data in a commonly used and machine-readable format. This right only applies to information that was collected using a basis of processing other than consent or contract. The controller must send the data to another controller upon request by the data subject. A data subject does not waive his/her right to erasure by requesting a portable version of the data. The controller has one month to respond to a data subject's request to exercise his/her rights. If the requests are multiple or complex, the controller can notify the data subject that it needs up to an additional two months. If possible and not otherwise requested by the data subject, the information in response to the request(s) is sent electronically. The controller has one month to tell a data subject it is not responding to his/her requests

	and explaining why. The controller must also tell the data subject about the right to complain to the supervisory authority and/or go to court.

Level HIPAA Implementation Requirements

Level HIPAA Implementation:	With limited exceptions, the organization provides individuals the right of access to review and obtain a copy of their PII (e.g., PHI in a designated record set for as long as the record set is maintained), and provides such access in a timely manner (e.g., 30 days with no more than one 30-day extension for a designated record set) for no more than a reasonable, cost-based fee, or, if the organization does not maintain or process the PII but knows where it's located or processed, the organization informs the individual where to direct the request. Where the individual makes the request, and unless otherwise requested by the individual, the organization provides the information in a structured, commonly used and machine readable (electronic) format. However, the organization also ensures the right to obtain a copy of this information does not adversely impact the rights and liberties of others. The covered entity provides the individual access to the PHI in the designated record set in a written or electronic form and format requested by the individual or otherwise agreed to by the covered entity and the individual. Summaries of the PHI requested are only provided in lieu of the designated record set if the individual agrees in advance to the summary and any fees imposed for providing such summary. The covered entity only provides access to another person designated by the individual if the individual requests such access in writing, signed by the individual, and the request clearly identifies the designated person and where the copy of the PHI is sent. The organization (e.g., an organization acting as a covered entity) formally verifies (e.g., with appropriate documentation) the identity and authority of persons (e.g., public officials) requesting covered and/or confidential information (e.g., PHI). The covered entity may deny an individual access to their PHI without providing an opportunity to review only for psychotherapy notes, information compiled in anticipation of legal proceedings or subject to, or exempt from, the Clinical Laboratory Improvements Amendments of 1988; the covered entity is a correctional facility; the individual is involved in research in progress; the information is contained in records subject to the Privacy Act; or the information was obtained from an entity other than a healthcare provider on the promise of confidentiality. Should a licensed healthcare professional determine that access would endanger the life or physical safety of, or otherwise cause substantial harm to, the individual or another person, access to the individual's PHI is denied. The covered entity provides timely (30 days plus no more than one 30-day extension), written denial to an individual's request for access in plain language that addresses the basis for denial, a statement of the individual's rights for review of the denial (e.g., review of the denial by a licensed healthcare professional), and a description of procedures for complaints to the entity and the Secretary of Health and Human Services. The organization ensures individuals have the right to amend PII (e.g., PHI or a record about the individual in a designated record set) for as long as the PII is maintained. The covered entity denies an individual's request for amendment only if it determines the PHI or record was not created by the covered entity (unless the originator no longer exists), is not part of the designated record set, is not available for inspection, or is otherwise accurate and complete. The covered entity acts on an individual's request for amendment within 60 days of the request, with no more than one 30-day extension.

	If the requested amendment is accepted in whole or in part, the organization makes the amendment, informs the individual the amendment was made in a timely manner, and makes reasonable efforts to notify relevant persons with whom the amendment must be shared in a reasonable timeframe. If a requested amendment is denied in whole or in part, the covered entity must provide the individual with a written denial; permit the individual to submit a statement of disagreement; prepare a written rebuttal if the individual submits a statement of disagreement; maintain denials, disagreements and rebuttals as organizational records; and provide relevant information regarding any disagreements in future disclosures of the individual's PHI. The covered entity corrects an individual's PHI if informed by another covered entity of an amendment. Persons and organizations ensure that communications between a patient and a healthcare professional are made available upon request. A covered entity may require the individual to make a request for a confidential communication in writing. Communication between a healthcare provider and a patient, and records of the identity, evaluation, or treatment of a patient, which are made or created in the course of providing healthcare services to the patient, are considered confidential and privileged and may not be disclosed, except as provided by federal or state law. The covered entity must permit, and must accommodate reasonable requests by, individuals who represent they are in danger to request to receive communications of PHI from the covered entity by alternative means or at alternative locations. As appropriate, the covered entity only conditions requests for confidential communications on how payment, if any, will be handled and the specification of an alternative address or other method of contact; however, in no case may the organization require an explanation as to the basis of the individual's request. The organization (i) publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records; (ii) publishes access procedures in System of Records Notices (SORNs); and (iii) adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

Objective Name: 13.03 Purpose Specification

Control Objective:	The authorities which permit the collection of PII and specifically the purpose(s) for which the PII is intended to be used are articulated.

Control Reference: 13.g Purpose Legitimacy

Control Specification:	To ensure that the purpose(s) for processing PII complies with applicable laws and relies on a permissible legal ground.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1	Applicable to all Organizations

Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to HITRUST De-ID Framework Requirements Subject to NIST SP 800-53 R4 (Privacy)
Level 1 Implementation:	The organization will determine the legal authority that permits the processing of PII, either generally or in support of a specific program or information system. The organization's purposes for processing PII will comply with applicable law, align with the collector's privacy notice, and rely on a permissible legal basis. Organizations will determine whether the proposed PII processing: 1. Can be initiated based on a legal ground other than consent (e.g., law enforcement, public safety, legal obligation or a legitimate interest of the PII controller). 2. Is governed by a legal ground that prohibits the data subject from exercising their choice regarding the processing of their PII. Organizations will develop and implement guidelines that ensures the processing of PII complies with all applicable laws and regulation and its interpretation by competent authorities. The overall context of the PII processing is considered when determining purpose legitimacy. This includes the relationship between the organization and the data subjects, scientific and technological developments, and social and cultural changes. Organizations will develop guidelines which safeguards the processing of PII and ensures that it is not carried out in a way which leave the PII unnecessarily vulnerable to a breach or potentially breaches any legal obligations, including statutory provisions, common law or contractual terms.
Level 1 Control Standard Mapping:	EU GDPR Article 5(1)(a) ISO/IEC 29100:2011 5.3 ISO/IEC 29151:2017 A.4.1 ISO/IEC 29151:2017 A.4.1(a) ISO/IEC 29151:2017 A.4.1(b) ISO/IEC 29151:2017 A.4.1(c) ISO/IEC 29151:2017 A.4.1(d) NIST SP 800-53 R4 AP-1[P]{0} NIST SP 800-53 R4 UL-2d[P]{0}

Level GDPR	**Implementation Requirements**
Level GDPR Implementation:	There are six legal bases for processing: consent; contract; compliance with legal obligation; vital interests of a natural person; in the public interest or in the exercise of official authority; or for legitimate interests. Processing that is limited to the scope of the data subject's consent is lawful. Member State law may require consultation with a supervisory authority if the processing is done in the public interest. Processing relating to criminal convictions or offenses may only be processed in accordance with EU or Member State law or under control of an official authority.

Level Personal Data Protection Act	**Implementation Requirements**
Level Personal Data Protection Act Implementation:	The Do Not Call Registry applies to messages offering, advertising, or promoting goods or services address to a Singapore telephone number if the person receiving the call is in Singapore when the message is left or received. A person must check the Do Not Call Register before attempting to call or send an applicable message. [PDP DNCR R 2013]. A person or entity must register to the PDPC

	to use the Do Not Call Register and update their contact information with the PDPC as necessary. A registered person or entity must apply to the PDPC to determine if a number is on the Do Not Call Register. The message must include the identification of the person or entity sending the message and contact information for the sender. It is assumed that this information will be valid for at least 30 days from the time of the message. Senders of messages may not block their own numbers.

Control Reference: 13.h Purpose Specification

Control Specification:	To specify the purposes for which PII are collected no later than at the time of PII collection where feasible and limit the subsequence use to the fulfillment of original purposes.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to EHNAC Accreditation Subject to NIST SP 800-53 R4 (Privacy)
Level 1 Implementation:	Where feasible, organizations will communicate to the data subject the purpose(s) of collection before PII is collected or used for the first time for a new purpose. Language which is clear and appropriately adapted to the circumstances is used and, if applicable, sufficient explanations provided for the need to process sensitive PII. Organizations will regularly review the purpose(s) for which PII is collected to ensure that they are still valid. Once the organization has identified the specific purposes, the purposes will be described clearly in the organization's related privacy compliance documentation and/or forms used to collect PII. Organizations will identify the PII useful to each business purpose and logically separate the PII useful to each business process. Organizations will regularly confirm the effective separation of PII and that no recipients and/or interconnections have been added.
Level 1 Control Standard Mapping:	ISO/IEC 29100:2011 5.3 ISO/IEC 29151:2017 A.4.2 ISO/IEC 29151:2017 A.4.2(a) ISO/IEC 29151:2017 A.4.2(b) ISO/IEC 29151:2017 A.4.2(d) ISO/IEC 29151:2017 A.5(f) NIST SP 800-53 R4 DI-1(1)[P]{0} NIST SP 800-53 R4 IP-1(1)[P]{0} NIST SP 800-53 R4 UL-1[P]{0} PDPA 14(1) PDPA 20(1)

Objective Name: 13.04 Data Minimization

Control Objective:	Only PII that is directly relevant and necessary to accomplish the specified purpose(s) is collected.

Control Reference: 13.i Collection Limitation

Control Specification:	To limit the collection of PII to that which is within the boundaries of applicable law and strictly necessary for the specified purpose(s).
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Privacy) Subject to Texas Health and Safety Code
Level 1 Implementation:	Organizations will ensure that the collection of PII is limited strictly to information that is relevant to the purpose(s) of collection and such information is only obtained by fair and lawful means. Where appropriate, notice is given to the data subject and/or consent from the data subject will be obtained. Organizations will not indiscriminately collect PII and will limit the amount of PII collection from and/or about the data subject from sources other than the data subject. Organizations will determine which PII needs to be collected to achieve its purpose before proceeding with the PII collection. Organizations will refrain from collecting PII which is sensitive, unless the collection of such information is legally authorized, or consent is obtained from the data subject. It is important to note that some jurisdictions may define certain categories of PII as sensitive and may impose restrictions and/or conditions on the collection of this PII. PII controllers take this into account when determining which PII they can collect and how it may be collected. Organizations will conduct an initial assessment of the PII they retain and establish and follow a schedule to regularly review such PII to ensure that only the PII which is identified in their notice is collected and its collection is necessary to accomplish their business purposes.
Level 1 Control Standard Mapping:	AICPA 2017 P2.1 AICPA 2017 P3.1 AICPA 2017 P4.1 APEC II 18 EU GDPR Article 5(1)(c) EU GDPR Recital 39 ISO/IEC 29100:2011 5.4 ISO/IEC 29151:2017 A.5 ISO/IEC 29151:2017 A.5(a) ISO/IEC 29151:2017 A.5(b) ISO/IEC 29151:2017 A.5(c) ISO/IEC 29151:2017 A.5(e) ISO/IEC 29151:2017 A.5(f) ISO/IEC 29151:2017 A.5(g) ISO/IEC 29151:2017 A.6(d) NIST SP 800-53 R4 DI-1(2)[P]{0} NIST SP 800-53 R4 DM-1(1)[P]{0} NIST SP 800-53 R4 DM-2(1)[P]{1} OECD Part 2 7 PDPA 18

Level GDPR Implementation Requirements

Level GDPR Implementation:	Personal data may be collected only for specific purposes and not processed beyond those purposes unless it is for archiving in the public interest or other select research purposes. A controller does not need to obtain or maintain personal data that is otherwise not needed solely for the purpose of complying with the GDPR.

Control Reference: 13.j Data Minimization

Control Specification:	To minimize the PII which is processed to what is strictly necessary for the legitimate interest pursued by the PII controller and to limit the disclosure of PII to a minimum number of internal and external parties.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to EHNAC Accreditation
Level 1 Implementation:	Organizations will use or offer, wherever possible, as default options, interactions and transactions which do not require the identification of the data subject and will limit the link-ability of the PII which they collect. Organizations will determine which of the PII they have collected is anonymized or pseudonymized based on the content, form the PII is stored and identified risks. PII that requires anonymization is anonymized based on the form of the PII and the identified risks. Pseudonymization means removing information from Personal Data that allows for a person to be identified without additional information and keeping that additional information separately. GDPR applies to pseudonymized data but not anonymized data. Appropriate safeguards must be in place for processing related to archiving in the public interest, scientific or historical research, or statistical purposes. Safeguards must ensure data minimization is respected and pseudonymization or anonymization is used when appropriate.
Level 1 Control Standard Mapping:	EU GDPR Article 4(5) EU GDPR Article 89(1) EU GDPR Recital 26 ISO/IEC 29100:2011 5.5 ISO/IEC 29151:2017 A.6(b) ISO/IEC 29151:2017 A.6(c) ISO/IEC 29151:2017 A.6(f) ISO/IEC 29151:2017 A.6(g)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions

	Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Privacy)
Level 2 Implementation:	The organization, where feasible, uses techniques (e.g., as described in NIST SP 800-122) to minimize the risk to privacy of using PII for research, testing, or training.
Level 2 Control Standard Mapping:	CMSRs v3.1 DM-03(01) (HIGH; MOD) De-ID Framework v1 Aggregated Data: Disclosure Policy MARS-E v2 DM-3(1) NIST SP 800-53 R4 DM-3(1)[P]{0} NIST SP 800-53 R4 DM-3[P]{0}

Level GDPR Implementation Requirements

Level GDPR Implementation:	Subject to certain exceptions, sensitive categories of personal data, which include race, ethnicity, political or religious beliefs, trade union membership, genetic information, biometric information, and information regarding the health or sex life or orientation of a person, is not to be processed. Special categories of information may be processed in accordance with certain exceptions, including consent, vital interests, employment issues, and several other reasons.

Level HIPAA Implementation Requirements

Level HIPAA Implementation:	The covered entity or business associate makes reasonable efforts to limit requests for PHI to, or from, another covered entity or business associate to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. Exceptions include, but are not limited to, treatment, requests by the individual, or uses or disclosures pursuant to a valid authorization, required by law, or required for compliance with other requirements, such as disclosures made to the Secretary of Health and Human Services. The covered entity only creates and uses information that is not individually identifiable (i.e., de-identified) when a code or other means of record identification designed to enable coded, or otherwise de-identified information to be re-identified, is not disclosed. If the de-identified information is subsequently re-identified, the covered entity only uses or discloses such re-identified information as permitted or required for PHI. The covered entity or business associate understands that health information is not identifiable (i.e., de-identified) only when there is no reasonable basis to believe that the information can be used to identify an individual and meets federal requirements for de-identified data. When de-identifying PHI, the covered entity removes all 18 data elements required by the HIPAA Administrative Simplification's Privacy Rule and has no knowledge the resulting data set could be re-identified, or an appropriate person applies generally accepting scientific principles and methods for rendering information not individually identifiable and determines the risk of re-identification is appropriately small. The covered entity may enter into a data use agreement with a recipient before allowing the use or disclosure of a limited data set and ensures the data provided meets the requirements for a limited data set.

	Unless otherwise allowed by relevant law, regulation, or contractual arrangement, the organization does not process PII revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, nor process genetic or biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation. The organization, where feasible and within the limits of technology, locates and removes/redacts specified PII and/or uses anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.

Objective Name: 13.05 Use Limitation

Control Objective:	PII is used solely for the purpose(s) specified in the privacy notice and only for a purpose that is compatible with the purpose for which the PII was collected.

Control Reference: 13.k Use and Disclosure

Control Specification:	To limit the use and disclosure of PII for specific, explicit and legitimate purposes and to fulfill the stated purpose(s) or to abide by applicable laws.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to HIPAA Security Rule Subject to NIST SP 800-53 R4 (Privacy) Subject to NY OHIP Moderate-Plus Security Baseline Subject to Texas Health and Safety Code
Level 1 Implementation:	Organizations will develop, document, and disseminate guidelines for the use and disclosure of PII. PII will only be used or disclosed for authorized purposes identified in the privacy notice or otherwise authorized by law. Organizations will evaluate new instances of use and disclosure to assess whether the use and disclosure is authorized or if new or additional consent and notice is required. Organizations will adopt a 'need-to-know' principle and make reasonable efforts to ensure that access to PII is given only to those who need it to conduct their official and legitimate duties. Organizations will restrict the disclosure of documents containing PII to a minimum necessary of stakeholders who need them in connection with their official and legitimate work duties. Organizations will only use and disclose PII for purposes the data subject has consented to. PII may only be used for purposes beyond that for which it was initially collected if the new purposes are compatible with the original purpose.
Level 1 Control Standard Mapping:	45 CFR Part § 164.308(a)(3)(ii)(B) HIPAA.SR-2 45 CFR Part § 164.514(d)(3) HIPAA.PR AICPA 2017 P6.1

	APEC IV 19 CMSRs v3.1 AP-01 (HIGH; MOD) CMSRs v3.1 IP-01 (HIGH; MOD) CMSRs v3.1 UL-01 (HIGH; MOD) EU GDPR Article 6(4) ISO/IEC 29100:2011 5.5 ISO/IEC 29100:2011 5.6 ISO/IEC 29151:2017 A.6(a) ISO/IEC 29151:2017 A.6(e) ISO/IEC 29151:2017 A.7.1(a) ISO/IEC 29151:2017 A.7.1(c) MARS-E v2 AP-1 MARS-E v2 AP-3 MARS-E v2 IP-1 MARS-E v2 UL-1 NIST SP 800-53 R4 AP-2[P]{0} NY DOH SSP v3.1 AC-2.IS.PII3[M]-0 NY DOH SSP v3.1 AC-2.IS.PII5[M]-0 NY DOH SSP v3.1 AC-3(9).IS.PII1[M]-3 OECD Part 2 10

Level 2	Implementation Requirements
Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Privacy) Subject to NY OHIP Moderate-Plus Security Baseline
Level 2 Implementation:	Organizations formally evaluate any proposed new uses of PII to assess whether they fall within the scope of the organizational authorities.
Level 2 Control Standard Mapping:	CMSRs v3.1 UL-01 (HIGH; MOD) CMSRs v3.1 UL-02 (HIGH; MOD) MARS-E v2 UL-1

Level De-ID Data Environment	Implementation Requirements
Level De-ID Data Environment Implementation:	Audits of the use and disclosure of covered information are regularly conducted, and any identified issues are remediated. The use or disclosure of covered information is monitored, and such monitoring is supported by automated alerting and response plans. The organization only publishes or discloses data that is de-identified for the intended context (environment), unless otherwise permitted by law.

Level EHNAC	Implementation Requirements

Level EHNAC Implementation:	The organization ensures all required uses and disclosures of PHI meet the implementation specifications listed in the HIPAA Privacy Rule. The organization ensures all permitted uses and disclosures of PHI meet the implementation specifications listed in the HIPAA Privacy Rule.

Level Federal Implementation Requirements

Level Federal Implementation:	A health plan that is a government program providing public benefits may disclose PHI relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing is required or expressly authorized by statute or regulation. A covered entity that is a government agency administering a government program providing public benefits may disclose PHI relating to the program to another covered entity that is a government agency administering a government program providing public benefits if they serve similar populations and the disclosure is necessary to coordinate the functions of such programs.

Level GDPR Implementation Requirements

Level GDPR Implementation:	Transfers from a public register can be made without the required safeguards as long as not all of the information is transferred and/or if the entity has a legitimate interest in the data. Public bodies may only transfer data under a derogation in the public interest, if necessary for a legal claim, if necessary to protect the vital interests of a natural person, or it is made from a public register. Derogations for the public interest relate to public interests expressed in EU or Member State law. Assessments made with respect to transfers made under approved derogations must be documented.

Level Group Health Plans Implementation Requirements

Level Group Health Plans Implementation:	The group health plan documents appropriately restrict the use and disclosure of PHI by the plan sponsor. The group health plan, or a health insurance issuer or HMO with respect to the group plan, limits disclosures to the plan sponsor of information on whether an individual is participating in the plan or is enrolled in or disenrolled from a health insurance issuer or HMO offered by the plan. The group health plan documents are amended as required to incorporate provisions to establish permitted and required uses and disclosures and disclose PHI to the plan sponsor only upon receipt of certification that the documents have been amended for specific, limited reasons (e.g., that no use or further disclosure other than that permitted or required will be made). Plan documents ensure adequate separation between the group health plan and the plan sponsor by describing employees or classes of employees to whom PHI may be disclosed, restricting access and use by such persons or classes of persons to the administrative functions the plan sponsor performs, and providing an effective mechanism for resolving issues of noncompliance with the plan document provisions.

Level HIPAA Implementation Requirements

Level HIPAA Implementation:	The covered entity limits permitted uses or disclosures of PHI to the individual; for treatment, payment or healthcare operations; incident to a use or disclosure otherwise permitted or required; or otherwise, pursuant to a valid authorization or agreement. The covered entity complies with the regulatory criteria for permitted uses and disclosures of PHI for public health activities for purposes including preventing or controlling disease; reporting incidents of child abuse or neglect; relating to the jurisdiction of the Food and Drug Administration; intervention or investigation of communicable diseases; work-related illness or injury; or to disclose proof of immunization. The covered entity discloses PHI about an individual whom the entity reasonably believes to be a victim of abuse, neglect, or domestic violence to government authorities authorized by law to receive such reports only to the extent necessary and required by law and notifies the individual when required by law. The covered entity discloses PHI to a health oversight agency only for those oversight activities authorized by law. The covered entity ensures that satisfactory assurances are obtained before providing the appropriate disclosures of PHI pursuant to court orders, subpoenas, or discovery requests for judicial and administrative proceedings. The covered entity only discloses PHI to law enforcement for valid law enforcement purposes when specifically, defined criteria are met. The covered entity limits disclosure of PHI to a coroner or medical examiner—or a covered entity acting in the capacity of a coroner or medical examiner—to that required to identify a decease person, determine a cause of death, or other duties as authorized by law. The covered entity limits disclosure of PHI to funeral directors, consistent with applicable law, to the minimum necessary to carry out their duties with respect to the decedent. The covered entity limits uses or discloses of PHI to legitimate organ procurement organizations for the purpose of facilitating organ, eye or tissue donation and transplantation. The covered entity uses or discloses PHI for research only if approved by a valid IRB or privacy board and receives appropriate representations from the research regarding the appropriate uses and disclosures necessary for research purposes. Documentation for a use or disclosure permitted for research based on approval of an alteration or waiver contains a signed, dated statement from the IRB or privacy board that confirms the necessary conditions for use or disclosure. A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose PHI to the extent allowed if the covered entity, in good faith, believes the use or disclosure is reasonable or necessary for safety or law enforcement. The covered entity discloses PHI to an individual when requested or required under federal or state law, or when required by the Secretary of Health and Human Services to investigate or determine the covered entity's compliance with the HIPAA Privacy Rule. The business associate discloses PHI when required by the Secretary of Health and Human Services to investigate or determine the business associate's compliance with the HIPAA Privacy Rule and to the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations as described in CSF control 13.f with respect to an individual's request for an electronic copy of PHI. A business associate only uses or discloses PHI as permitted or required by its business associate contract or other arrangement and does not use or disclose PHI in a manner that would violate requirements for the protection of such information, if done by the

	covered entity, except for the purposes specified in CSF control 13.f if such uses or disclosures are permitted by its contract or other arrangement. An organization may disclose covered and/or confidential information (e.g., PHI) to a service provider (e.g., a business associate) and may allow a service provider to, receive, maintain, or transmit covered and/or confidential information on its behalf, if the organization obtains satisfactory, written assurance (e.g., a written contract, agreement or arrangement that satisfies the requirements of this control) that the service provider will appropriately safeguard the information. The covered entity expressly permits disclosures of PHI by whistleblowers and specifies the appropriate conditions under which whistleblowers may disclose PHI. The covered entity permits certain disclosures of PHI by workforce members who are victims of a crime to law enforcement and specifies the conditions under which they may disclose PHI. The covered entity only uses or discloses specific, limited types of PHI under specific, defined conditions to a business associate or an institutionally-related foundation for the purpose of raising funds for its own benefit. The covered entity restricts uses and/or disclosures of PHI used for underwriting purposes for any other purpose except as may be required by law. Unless the entity is an issuer of long-term care policies, the health plan may not use or disclose PHI that is genetic information for underwriting purposes. The covered entity or business associate cannot sell PHI. If the covered entity has multiple functions that would make the entity any combination of a healthcare provider, a health plan, and a healthcare clearinghouse, it ensures the use and disclosure of PHI is only for the purpose related to the appropriate function being performed. If the covered entity discloses PHI to a family member, or other relative, or a close personal friend of the individual, or any other person identified by the individual, or to assist and locate such a person, the disclosure is limited to that PHI directly relevant to the person's involvement with the individual's care or payment related to such care, or otherwise limited to the requirements for limited uses and disclosures when the individual is not present, for disaster relieve purposes, or for a deceased individual. When an individual is not present or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of incapacity or emergency, the covered entity ensures that it only allows uses or provides disclosures of PHI to a person that is directly relevant to that person's involvement with the individual's health care. The covered entity limits disclosure of PHI to a public or private entity authorized by law or by its charter, to assist in disaster relief efforts or emergency response. If the individual is deceased, a covered entity only discloses to a family member, or other persons who were involved in the individual's care or payment for health care prior to the individual's death, PHI of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any known prior expressed preferences. A covered entity may use or disclose a limited data set only for the purposes of research, public health, or healthcare operations. In certain instances, an organization uses or discloses protected health information (i) without the written authorization of the individual or the opportunity for the individual to agree or object, and (ii) to the extent that such use or disclosure is required by law and the use or disclosure complies with, and is limited to, the relevant requirements of such law.

	The organization disclose PHI to law enforcement for identification and location purposes subject to specifically defined criteria, including whether or not notice or consent is provided. The organization discloses PHI related to victims of a crime to law enforcement subject to specifically defined criteria. The organization discloses PHI related to an individual who has died to law enforcement subject to specifically defined criteria. The organization discloses PHI related to a crime on premises or in an emergency to law enforcement subject to specifically defined criteria. The organization uses or discloses the PHI of Armed Forces personnel for activities deemed necessary by appropriate military command authorities only if the authority has published notice in the Federal Register with specific, required information. The organization disclose PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities. The organization disclose PHI to authorized Federal officials for the provision of protective services to authorized officials or for the conduct of authorized investigations. An organization that is a component of the Department of State uses PHI only to make determinations regarding the medical suitability of an individual to officials in the Department of State who need access to such information for specific, defined purposes. The organization uses or discloses PHI of an inmate to a law enforcement official having lawful custody of the inmate if the correctional institution or such law enforcement official represents such PHI is necessary for specific, defined requirements. The organization only discloses PHI as authorized and to the extent necessary to comply with laws relating to workers' compensation or similar programs. The organization uses or discloses PII for research only if approved by a valid IRB or privacy board and receives appropriate representations from the researcher regarding the appropriate uses and disclosures necessary for research purposes. Documentation for a use or disclosure permitted for research based on approval of an alteration or waiver contain a signed, dated statement from the IRB or privacy board that confirms the necessary conditions for use or disclosure.
Level Personal Data Protection Act	**Implementation Requirements**
Level Personal Data Protection Act Implementation:	Data may only be transferred outside Singapore if adequate protections are in place for the data unless the organization has obtained an exemption from the PDPC. Controllers must have reasonable security measures in place to prevent unauthorized disclosures and related risks.
Level Texas Covered Entities	**Implementation Requirements**
Level Texas Covered Entities Implementation:	Sensitive personal information obtained by or through state agencies are not subject to subpoena except as authorized by law. Genetic information about an individual is only disclosed to the individual, a physician designated by the individual in writing, or another person or agency as provided by applicable state and federal law.

	Information related to a survivor of sexual assault, or the victimization of a survivor, is confidential and not disclosed except as provided by law. The section of a birth certification entitled For Medical and Health Use Only is confidential and not disclosed or made public on subpoena, except as provided by law. Information relating to cases or suspected cases of diseases or health conditions is confidential and not disclosed or made public on subpoena except as provided by law. Morbidity reports are confidential and not disclosed except as provided by law. Reports of abuse, neglect or exploitation of minor, elderly and disabled persons, information related to the investigation, or information in providing services as a result of an investigation are confidential and not disclosed except as provided by law. Occupational health case reports are confidential and not disclosed except as provided by law. Reports of abuse, neglect or exploitation of persons with an intellectual disability or related conditions (ICF/IID), information related to the investigation, or information in providing services as a result of an investigation are confidential and not disclosed except as provided by law. Reports of abuse, neglect or exploitation of persons by a chemical dependency counselor or treatment center, information related to the investigation, or information in providing services as a result of an investigation are confidential and not disclosed except as provided by law. Medicaid information is not disclosed except as provided by state law. Information concerning quality of care at end stage renal facilities are confidential and not subject to disclosure, subpoena, discovery or other compulsory legal process. Records relating to resident deaths are confidential and not subject to release or disclosure except as provided by law. Alcohol and drug abuse patient records maintained in connection with any federally assisted alcohol and drug abuse program are confidential and disclosed only as permitted by federal law. Patient communications with and records maintained by a dentist are confidential and may not be disclosed except as provided by law. Patient communications with, and records maintained by, a physician are confidential and may not be disclosed except as provided by law. Patient communications with, and records maintained by, a chiropractor are confidential and may not be disclosed except as provided by law. Patient communications with, and records maintained by, a podiatrist are confidential and may not be disclosed except as provided by law. Communications with patients or clients related to any mental or emotional condition or disorder require special handling and are only disclosed as permitted by law. Medicaid information is not disclosed except as provided by federal law. Individually identifiable immunization information sent to, or received by, the TX state registry is only disclosed to the individual or legally authorized representative except as provided by law.

	Requests for information from the state immunization registry is only made with the written consent of the individual or authorized representative and is not disclosed or made public on subpoena except as provided by law. Family planning information is confidential and is not disclosed without written authorization except as provided by law. Government benefit and federal assistance information is confidential and not disclosed without written authorization except as provided by law. A hospital or an agent or employee of a hospital may not disclose healthcare information without written authorization except as provided by law. Cancer data is released to the TX Cancer Registry with or without patient authorization. No part of a medical record received from the Social Security Administration is withheld from the patient, parent or guardian, as applicable. Laboratories maintain the confidentiality and accuracy of patient information, transmit test results in a timely manner, and only disclose patient information as permitted by law. Genetic test results are only disclosed to the individual or a physician designated by the individual upon written request.

Control Reference: 13.l Retention and Disposal

Control Specification:	To retain PII no longer than necessary to fulfill the stated purpose(s) or to abide by applicable laws.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation:	Organizations will limit the retention of PII to only that which is deemed necessary and for as long as necessary to fulfill the organization's specific and legitimate purpose and/or required by law. Unless certain exceptions apply, PII must be deleted thereafter. Organizations will ensure that retention periods are appropriately followed and PII is disposed of in accordance with the defined retention periods. Regardless of the method of storage, organizations will destroy, erase, dispose, sanitize, and/or anonymize the PII in a manner which prevents PII from being lost, stolen, misused or accessed without authorization once the PII is no longer needed for the stated purpose for which it was collected and/or at the end of the applicable legally required retention period.
Level 1 Control Standard Mapping:	AICPA 2017 C1.2 AICPA 2017 P3.2 AICPA 2017 P4.2 AICPA 2017 P4.3 EU GDPR Article 5(1)(e)

	EU GDPR Recital 39 ISO/IEC 29100:2011 5.6 ISO/IEC 29151:2017 A.7.1(a) ISO/IEC 29151:2017 A.7.1(d) ISO/IEC 29151:2017 A.7.1(e) ISO/IEC 29151:2017 A.7.1(i) NIST SP 800-53 R4 DM-2(1)[P]{3} NIST SP 800-53 R4 DM-2a[P]{0} NIST SP 800-53 R4 DM-2b[P]{0} NY DOH SSP v3.1 MP-6.PII1[M]-2 PDPA 25

Level Group Health Plans Implementation Requirements

Level Group Health Plans Implementation:	Amended plan documents are subject to the organization's retention policy.

Objective Name: 13.06 Data Quality and Integrity

Control Objective:	PII is relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, is accurate, complete and kept up-to-date.

Control Reference: 13.m Accuracy and Quality

Control Specification:	To ensure that the PII processed is accurate, complete, up-to-date, adequate and relevant for the purpose of use.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation:	To achieve data quality, organizations must ensure that PII is being accurately processed, complete, up-to-date, adequate, and relevant for the organization's purpose of use. If it is not, it must be erased or edited. Organizations will establish collection guidelines to ensure the quality and accuracy of PII. Upon collection or creation of PII, organizations, where practicable, will confirm the accuracy, relevance and completeness of the PII. Organizations will check applicable programs or systems for inaccurate or outdated PII and correct as necessary.
Level 1 Control Standard Mapping:	AICPA 2017 P1.1 AICPA 2017 P6.2 AICPA 2017 P7.1 APEC VI 21 EU GDPR Article 5(1)(d) ISO/IEC 29100:2011 5.7 ISO/IEC 29151:2017 A.8 ISO/IEC 29151:2017 A.8(a) ISO/IEC 29151:2017 A.8(c) ISO/IEC 29151:2017 A.8(f)

	OECD Part 2 8 PDPA 23

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Privacy)
Level 2 Implementation:	The organization requests that the individual or individual's authorized representative (i) validate PII during the collection process, and (ii) periodically revalidate that PII collected is still accurate at an organization-defined frequency but no less than annually. The organization establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act. The organization publishes Computer Matching Agreements on its public website.
Level 2 Control Standard Mapping:	CMSRs v3.1 DI-01(01) (HIGH; MOD) CMSRs v3.1 DI-01(02) (HIGH; MOD) CMSRs v3.1 DI-02 (HIGH; MOD) CMSRs v3.1 DI-02(01) (HIGH; MOD) MARS-E v2 DI-1(1) MARS-E v2 DI-1(2) MARS-E v2 DI-2 MARS-E v2 DI-2(1) NIST SP 800-53 R4 DI-2(1)[P]{0} NIST SP 800-53 R4 DI-2b[P]{0}

Control Reference: 13.n Participation and Redress

Control Specification:	To provide any amendment, correction or removal to PII processors and third-parties to whom personal data had been disclosed.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to CCPA Requirements Subject to NIST SP 800-53 R4 (Privacy)

Level 1 Implementation:	Organizations will ensure that data subjects have the ability to challenge the accuracy of applicable PII and, where reasonable and appropriate, have the information amended or deleted. PII controllers will establish a process for data subjects to have PII maintained by the PII controller corrected or amended and disseminate corrections or amendments of PII-to-PII processors and other authorized users of the PII.
Level 1 Control Standard Mapping:	45 CFR Part § 164.526(a)(1) HIPAA.PR 45 CFR Part § 164.526(b)(1) HIPAA.PR 45 CFR Part § 164.526(f) HIPAA.PR AICPA 2017 P4.3 AICPA 2017 P5.2 APEC VIII 23(c) CCPA 1798.105(a) CMSRs v3.1 IP-03 (HIGH; MOD) ISO/IEC 29151:2017 A.10.2 MARS-E v2 IP-3 NIST SP 800-53 R4 IP-3[P]{0} PDPA 22(2)(b)

Level GDPR Implementation Requirements

Level GDPR Implementation:	The data subject has the right to have his/her information deleted or erased with undue delay upon request if the data is no longer needed, if consent is withdrawn, if the data subject objects to the processing and there is no overriding legitimate reason to keep it, the information was unlawfully processed, the information must be addressed to comply with an EU or Member State law, or if the data was collected from a child by an online entity. If the controller has made the data the subject seeks to have erased public, the controller needs to take reasonable means to inform other controllers of the erasure request and have any online links or copies deleted as well. Erasure is not required if the data processing is needed to exercise the right of freedom of expression or information, to comply with a legal obligation done in the public interest or in the exercise of governmental authority, for public health reasons, or archiving in the public interested or other similar research, or to establish or defend against legal claims. The controller must notify anyone to whom it has released any data following any rectification or erasure of data unless that is impossible or overly burdensome. In those cases, the controller must tell the data subject about those recipients if requested. If the relevant data was collected in order to carry out a task in the public interest or under official authority, or the processing was necessary for the legitimate interests of the controller or a third-party, the data subject has the right to object to such processing and any profiling done on the basis thereof. Unless the controller has or identifies a compelling reason to keep processing the data that overrides the concerns of the data subject, the controller must stop processing the data.

Level Group Health Plans Implementation Requirements

Level Group Health Plans Implementation:	The group health plan limits exceptions to the general requirements for amendments to PHI to health benefits provided other than solely through an insurance contract with a health insurance issuer or HMO and PHI that it does not create or receive, except for summary health information or information on whether the individual is participating in the group health plan or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

Control Reference: 13.o Complaint Management

Control Specification:	To set up efficient internal complaint handling and redress procedures for use by data subjects.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Privacy)
Level 1 Implementation:	Organizations will implement an efficient internal complaint management process for data subjects to use. A point of contact is tasked with receiving and responding to complaints, concerns, or questions from data subjects regarding the organization's privacy practices, policies and procedures. The organization's complaint management process will provide complaint mechanisms that: 1. Are easily accessible; 2. Easy to use; and 3. Contains all relevant information for filling complaints. The complaint management process will include tracking mechanisms to ensure that complaints are reviewed appropriately and addressed in a timely manner. Additionally, the process will also include corrective actions.
Level 1 Control Standard Mapping:	45 CFR Part § 164.530(d) HIPAA.PR AICPA 2017 P8.1 CMSRs v3.1 IP-04 (HIGH; MOD) CMSRs v3.1 IP-04(01) (HIGH; MOD) De-ID Framework v1 Complaints: Policy ISO/IEC 29100:2011 5.10 ISO/IEC 29151:2017 A.10.3 MARS-E v2 IP-4 MARS-E v2 IP-4(1) NIST SP 800-53 R4 IP-4(1)[P]{0} NIST SP 800-53 R4 IP-4[P]{0} PDPA 12(b)

Objective Name: 13.07 Accountability & Auditing

Control Objective:	The organization is accountable for complying with applicable privacy protection requirements.

Control Reference: 13.p Governance

Control Specification:	To establish efficient governance for PII processing.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to NY OHIP Moderate-Plus Security Baseline
Level 1 Implementation:	The organization will develop a comprehensive privacy governance program to ensure the compliance with applicable laws and regulations regarding the processing of PII by programs and systems. The program will be tailored to meet the structure, scale, volume, and sensitivity of the organization's operations and updated periodically. The performance of the program will also be periodically monitored. There will be an appointment of a person responsible, such as a data protection officer or privacy officer, who will be responsible for the organization's individual privacy protection program, and the officer will report directly to the highest management level of the organization (e.g., a CEO). The data protection officer will be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfill required tasks. The required expertise will vary depending on the processing the entity does, and the risks involved. Data protection officers must be able to act independently. Responsibilities will include the development and implementation of privacy policies and procedures, serving as the point of contact for all privacy-related complaints, and will provide privacy-related guidance to managers, users, and service providers on their individual responsibilities and the specific procedures that will be followed. The data protection officer will, in the performance of those tasks, have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing. The data protection officer may fulfill other tasks and duties; however, the organization ensures that any such tasks and duties do not result in a conflict of interests. The PII controller and PII processor will designate a data protection officer in any case where: 1. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; 2. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or 3. the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences. The organization supports the data protection officer in performing the tasks required by law or regulation by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain data protection officer's expert knowledge. The organization ensures that the data protection or privacy officer does not receive any instructions regarding the exercise of those tasks, and the officer will be bound by secrecy or confidentiality concerning the performance of those tasks, in accordance with applicable law or regulation. The officer will not be dismissed or penalized by the organization for performing those tasks.
Level 1 Control Standard Mapping:	EU GDPR Article 37(1) EU GDPR Article 37(5) EU GDPR Article 38(2) EU GDPR Article 38(3) EU GDPR Article 38(4)

	EU GDPR Article 38(5) EU GDPR Article 38(6) EU GDPR Article 39(1) EU GDPR Article 39(2) EU GDPR Article 5(2) EU GDPR Recital 97 ISO/IEC 29100:2011 5.10 ISO/IEC 29151:2017 A.11.1(e) ISO/IEC 29151:2017 A.11.1(h) NY DOH SSP v3.1 PM-2.IS.PHI1[M]-2 OECD Part 3 15(ii) PDPA 11(3)

Level GDPR Implementation Requirements

Level GDPR Implementation:	Controllers or their representative must maintain adequate records and logs of processing activities. Records or logs of processing must be in writing and must be available to supervisory authorities. Entities with less than 250 employees do not need to keep the same level of processing records as those with more employees unless data is processed on a regular basis, or the data processed is particularly sensitive. In determining the appropriate supervisory authority, a controller's main establishment in the EU is where its central administration is located or, if different, where decisions regarding processing data are made. A processor's main establishment in the EU is where its central administration is located or, if none, where processing occurs. Adequate binding corporate rules must include at least the information detailed in GDPR Article 47(2). Controllers and processors must adequately respond to decisions made by the lead supervisory authority in cases where more than one supervisory authority has jurisdiction. The controller or processor will inform the lead supervisory authority of the actions taken.

Control Reference: 13.q Privacy and Impact Assessment

Control Specification:	To establish a privacy impact assessment process and to perform a privacy impact assessment as necessary.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Privacy)
Level 1 Implementation:	The organization will conduct privacy impact assessments for systems, programs, or other activities that pose a privacy risk before developing or procuring information technology that collects, maintains, or disseminates PII in an identifiable form. Privacy impact assessments will additionally be conducted before initiating a new collection of PII that will be collected, maintained, or disseminated using information technology, and includes PII that permits the physical or online contacting of a specific data subject.

Level 1 Control Standard Mapping:	AICPA 2017 P8.1 NIST SP 800-53 R4 AR-4[P]{0}

Level GDPR Implementation Requirements

Level GDPR Implementation:	Prior to engaging in a new type of processing or processing using a new system, if there is a high risk involved and a breach occurs, the controller must carry out a data protection impact assessment. Processors assist controllers as appropriate with data protection impact assessments and any resulting implementation. If the controller has a data protection officer, the officer must be consulted on the data protection impact assessment. Data protection impact assessments are particularly needed if automated processing that will have a legal impact on data subject is occurring, the processing is on a large scale and includes sensitive data, or there is systemic, large-scale monitoring of a public area. If appropriate, a controller consults data subjects or their representatives in developing a data protection impact assessment. A data protection impact assessment is not needed if processing is done to comply with a legal obligation or for a task carried out in the public interest or in the exercise of official authority and a data protection impact assessment has already been done by the Member State as part of the adoption of the relevant legal basis. If there is a change to the risk involved, a controller reviews its data protection impact assessment accordingly. Before engaging in high-risk processing, as determined by a data protection impact assessment, a controller must consult its supervisory authority.

Control Reference: 13.r Privacy Requirements for Contractors and Processors

Control Specification:	To ensure, through contractual or other means, that third party recipients provide at least equivalent levels of PII protection.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Privacy) Subject to NY OHIP Moderate-Plus Security Baseline
Level 1 Implementation:	To ensure that third-party recipients provide adequate levels of privacy, PII controllers will establish PII protection rules and responsibility requirements for the PII processor and document within contracts, either directly or through reference to polices or another agreement, the PII protection requirements that PII processors are required to meet. PII controllers will document and communicate, as appropriate, all related policies, procedures and practices. Requirements for the use of subcontractors to process PII will be specified in the contract between the PII processor and the PII controller. PII controllers and PII processors will agree via contractual means that PII is not shared with third-parties without advanced notice, unless specifically permitted in the contract. A confidentiality

	clause will be included, binding both upon the provider and any of its employees who may be able to access the PII. PII processors will allow PII controllers to conduct audits to ensure the appropriate and continued implementation of PII protection requirements. PII controllers will specify to PII processors the conditions under which PII will be returned or appropriately disposed of upon completion of the service, termination of any governing agreement, or upon the request of the PII controller. PII controllers will provide clear expectations and responsibilities to the PII processors on the procedures to notify the PII controller in the event of a data breach that affects PII.
Level 1 Control Standard Mapping:	45 CFR Part § 164.504(e) HIPAA.PR AICPA 2017 P6.1 AICPA 2017 P6.5 AICPA 2017 P6.6 EU GDPR Article 28(3) EU GDPR Article 28(9) ISO/IEC 29100:2011 5.10 ISO/IEC 29151:2017 A.11.3(a) ISO/IEC 29151:2017 A.11.3(b) ISO/IEC 29151:2017 A.11.3(c) ISO/IEC 29151:2017 A.11.3(e) ISO/IEC 29151:2017 A.11.3(f) ISO/IEC 29151:2017 A.11.3(g) ISO/IEC 29151:2017 A.11.3(h) ISO/IEC 29151:2017 A.11.3(j) ISO/IEC 29151:2017 A.7.5 NIST SP 800-53 R4 AR-3a[P]{0} NIST SP 800-53 R4 UL-2b[P]{0} NY DOH SSP v3.1 AC-3(9).IS.PII1[M]-1

Level GDPR Implementation Requirements

Level GDPR Implementation:	Processors must maintain adequate records and logs of processing activities in which it engages. Controllers may only use processors who agree to adequately protect personal data. Processors can only process data pursuant to the instructions of a controller unless required to do so by EU or Member State law. Processors need written approval from controllers before subcontracting any processing. If the processor subcontracts any processing, the contract between the two processors must have the same protections as the contract between the controller and the original processor.

Level HIPAA Implementation Requirements

Level HIPAA Implementation:	The covered entity ensures each of its business associates have a valid agreement that addresses the proper management/oversight of the business associate and specifies applicable requirements (e.g., around use, further disclosure, and the implementation of reasonable and appropriate safeguards). In an arrangement between business associate and a subcontractor who handles PHI for the business associate, the contractual requirements apply in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate. The covered entity or business associate understands when it has not obtained satisfactory assurances or met the standards for business associate contracts and takes

	appropriate action if it knew of a pattern or activity or practice of the business associate that constituted a material breach or violation of its obligations.

Level NYDOH Implementation Requirements

Level NYDOH Implementation:	Systems processing, storing, or transmitting PII (to include PHI): When acquiring information systems, components, or services used to store, process, or transmit personally identifiable information (PII), ensure the following, in consultation with the privacy office, are included in the acquisition contract: (i) a list of security and privacy controls necessary to ensure protection of PII and, if appropriate, enforce applicable privacy requirements; (ii) privacy requirements set forth in Appendix J of NIST SP 800-53, Rev. 4, including privacy training and awareness, and rules of behavior; (iii) privacy functional requirements, i.e., functional requirements specific to privacy; and (iv) Federal Acquisition Regulation (FAR) Clauses per FAR Part 24 (clauses 52.224-1, Privacy Act Notification, and 52.224-2, Privacy Act. and Part 39 (clauses 39.105, Privacy, and 39.116, Contract clause), and any other organization-specific privacy clauses.

Control Reference: 13.s Privacy Monitoring and Auditing

Control Specification:	To monitor and audit PII protection controls and the effectiveness of internal PII protection policy.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation:	To verify that PII processing is conducted in a manner which meets data protection and privacy safeguarding requirements, organizations will regularly conduct audits and maintain documentation to demonstrate compliance. Organizations will ensure that all audits are conducted by qualified and independent parties, regardless of whether done internally or externally of the organization. If conducting audits with internal resources, organizations will periodically have an external party conduct the audit for an independent assessment.
Level 1 Control Standard Mapping:	AICPA 2017 CC4.1 AICPA 2017 P8.1 ISO/IEC 29100:2011 5.12 ISO/IEC 29151:2017 A.11.4(a) ISO/IEC 29151:2017 A.11.4(c) ISO/IEC 29151:2017 A.11.4(d)

Control Reference: 13.t Privacy Protection Awareness and Training

Control Specification:	To provide suitable training and awareness concerning PII protection for the personnel of the PII controller who will have access to PII.

Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	
Level 1 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Privacy) Subject to NY OHIP Moderate-Plus Security Baseline
Level 1 Implementation:	Organizations will develop, implement, and maintain a comprehensive privacy protection awareness and training program, organized to educate relevant personnel on their responsibilities of protecting PII and organizational procedures. Training will be administered at both a basic and targeted role-based level and completed on a regular basis or as required. Guidelines will be created to ensure relevant personnel are kept up-to-date on PII protection responsibilities, developments in regulations, contracts, and technologies that could impact PII or organizational privacy compliance. Organizations will ensure that after substantial updates, personnel periodically acknowledge and agree to adhere to their responsibilities for PII protection requirements. Organizations will develop, document, and implement remediation actions for violations of the privacy protection awareness and training policies.
Level 1 Control Standard Mapping:	ISO/IEC 29100:2011 5.10 ISO/IEC 29151:2017 A.11.5(a) ISO/IEC 29151:2017 A.11.5(b) ISO/IEC 29151:2017 A.11.5(c) ISO/IEC 29151:2017 A.11.5(d) NIST SP 800-53 R4 AR-5[P]{1} NIST SP 800-53 R4 AR-5[P]{2} NIST SP 800-53 R4 UL-2c[P]{0} NY DOH SSP v3.1 AC-2.IS.PII6[M]-2 NY DOH SSP v3.1 AT-3.IS.PII1[HM]-0

Level CCPA Implementation Requirements

Level CCPA Implementation:	Businesses ensure that individuals responsible for handling consumer inquiries are aware of all relevant requirements.

Control Reference: 13.u Privacy Protection Reporting

Control Specification:	To develop, disseminate and update PII protection reports.
Factor Type:	Organizational
Topics:	

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all Organizations
Level 1 System Factors:	

Level 1 Regulatory Factors:	
Level 1 Implementation:	Organizations will promote accountability and transparency in their PII protection operations by utilizing PII compliance reporting and external reporting as and when appropriate.
Level 1 Control Standard Mapping:	ISO/IEC 29151:2017 A.11.6

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Bed: Between 200 and 750 Beds Health Plan/Insurance/PBM: Between 1 million to 7.5 Million Lives HIE Transactions: Between 1 and 6 Million Transactions Hospital Admissions: Between 7.5k and 20k Patients IT Service Provider: Between 15 and 60 Terabytes(TB) Non-IT Service Provider: Between 25 and 100 Megabytes(MB) Pharmacy Companies: Between 10 million to 60 million Prescriptions Physician Count: Between 11 and 25 Physicians Physician Encounters: Between 60k to 180k Encounters Record Count Annual: Between 180k and 725k Records Record Total: Between 10 and 60 Million Records
Level 2 System Factors:	
Level 2 Regulatory Factors:	Subject to NIST SP 800-53 R4 (Privacy)
Level 2 Implementation:	The organization will develop, disseminate, and update privacy reports to appropriate oversight bodies to demonstrate accountability with statutory and regulatory privacy program mandates, as well as to privacy officials and other personnel with responsibility for monitoring privacy program progress and compliance.
Level 2 Control Standard Mapping:	NIST SP 800-53 R4 AR-6[P]{0}