

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2025.3
STRM Guidance: <https://securecontrolsframework.com/set-theory-relationship-mapping-strm/>

Focal Document:

Focal Document URL:
Published STRM URL:

HIPAA Security Rule & NIST SP 800-66 R2

<https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf>
<https://securecontrolsframework.com/content/strm/scf-strm-us-fed-hipaa-hitech.pdf>

| HIPAA-HITECH FDE # | NIST SP 800-66 R2 | HIPAA-HITECH FDE Name | HIPAA-HITECH Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship (optional) | Notes (optional) |
|----------------------|-------------------|-----------------------------------|--|----------------|-------------------|--|----------|---|-------------------------------------|------------------|
| § 164.306 | N/A | Security standards: General rules | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.306(a) | N/A | General requirements | Covered entities and business associates must do the following: | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.306(a)(1) | N/A | N/A | Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. | Functional | Subset Of | Cybersecurity & Data Protection Governance Program | GOV-01 | Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. | 10 | |
| § 164.306(a)(1) | N/A | N/A | Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. | Functional | Subset Of | Operationalizing Cybersecurity & Data Protection Practices | GOV-15 | Mechanisms exist to compel data and/or process owners to operationalize cybersecurity and data protection practices for each Technology Asset, Application and/or Service (TAAS) under their control. | 10 | |
| § 164.306(a)(1) | N/A | N/A | Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. | Functional | Subset Of | Select Controls | GOV-15.1 | Mechanisms exist to compel data and/or process owners to select required cybersecurity and data protection controls for each Technology Asset, Application and/or Service (TAAS) under their control. | 10 | |
| § 164.306(a)(1) | N/A | N/A | Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. | Functional | Subset Of | Implement Controls | GOV-15.2 | Mechanisms exist to compel data and/or process owners to implement required cybersecurity and data protection controls for each Technology Asset, Application and/or Service (TAAS) under their control. | 10 | |
| § 164.306(a)(1) | N/A | N/A | Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. | Functional | Subset Of | Assess Controls | GOV-15.3 | Mechanisms exist to compel data and/or process owners to assess if required cybersecurity and data protection controls for each Technology Asset, Application and/or Service (TAAS) under their control are implemented correctly and are operating as intended. | 10 | |
| § 164.306(a)(1) | N/A | N/A | Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. | Functional | Subset Of | Authorize Technology Assets, Applications and/or Services (TAAS) | GOV-15.4 | Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control. | 10 | |
| § 164.306(a)(1) | N/A | N/A | Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. | Functional | Subset Of | Monitor Controls | GOV-15.5 | Mechanisms exist to compel data and/or process owners to monitor Technology Assets, Applications and/or Services (TAAS) under their control on an ongoing basis for applicable threats and risks, as well as to ensure cybersecurity and data protection controls are operating as intended. | 10 | |
| § 164.306(a)(2) | N/A | N/A | Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. | Functional | Subset Of | Cybersecurity & Data Protection Governance Program | GOV-01 | Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. | 10 | |
| § 164.306(a)(3) | N/A | N/A | Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part. | Functional | Subset Of | Risk Management Program | RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. | 10 | |
| § 164.306(a)(3) | N/A | N/A | Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part. | Functional | Subset Of | Cybersecurity & Data Protection Governance Program | GOV-01 | Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. | 10 | |
| § 164.306(a)(3) | N/A | N/A | Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part. | Functional | Subset Of | Data Protection | DCH-01 | Mechanisms exist to facilitate the implementation of data protection controls. | 10 | |
| § 164.306(b) | N/A | Flexibility of approach | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.306(b)(1) | N/A | N/A | Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. | Functional | Intersects With | Define Control Objectives | GOV-09 | Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system. | 5 | |
| § 164.306(b)(1) | N/A | N/A | Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. | Functional | Subset Of | Operationalizing Cybersecurity & Data Protection Practices | GOV-15 | Mechanisms exist to compel data and/or process owners to operationalize cybersecurity and data protection practices for each Technology Asset, Application and/or Service (TAAS) under their control. | 10 | |
| § 164.306(b)(1) | N/A | N/A | Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. | Functional | Subset Of | Secure Engineering Principles | SEA-01 | Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS). | 10 | |
| § 164.306(b)(1) | N/A | N/A | Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. | Functional | Intersects With | Alignment With Enterprise Architecture | SEA-02 | Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity and data protection principles that addresses risk to organizational operations, assets, individuals, other organizations. | 5 | |
| § 164.306(b)(1) | N/A | N/A | Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. | Functional | Intersects With | Defense-In-Depth (DiD) Architecture | SEA-03 | Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers. | 3 | |
| § 164.306(b)(2) | N/A | N/A | In deciding which security measures to use, a covered entity or business associate must take into account the following factors: | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.306(b)(2)(i) | N/A | N/A | The size, complexity, and capabilities of the covered entity or business associate. | Functional | Intersects With | Defining Business Context & Mission | GOV-08 | Mechanisms exist to define the context of its business model and document the organization's mission. | 5 | |
| § 164.306(b)(2)(i) | N/A | N/A | The size, complexity, and capabilities of the covered entity or business associate. | Functional | Intersects With | Business Process Definition | PRM-06 | Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained. | 5 | |
| § 164.306(b)(2)(ii) | N/A | N/A | The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities. | Functional | Intersects With | Cybersecurity & Data Protection Requirements Definition | PRM-05 | Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC). | 5 | |
| § 164.306(b)(2)(ii) | N/A | N/A | The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities. | Functional | Intersects With | Alignment With Enterprise Architecture | SEA-02 | Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity and data protection principles that addresses risk to organizational operations, assets, individuals, other organizations. | 5 | |
| § 164.306(b)(2)(iii) | N/A | N/A | The costs of security measures. | Functional | Subset Of | Allocation of Resources | PRM-03 | Mechanisms exist to identify and allocate resources for management, operational, technical and data privacy requirements within business process planning for projects / initiatives. | 10 | |
| § 164.306(b)(2)(iv) | N/A | N/A | The probability and criticality of potential risks to electronic protected health information. | Functional | Subset Of | Risk Management Program | RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. | 10 | |
| § 164.306(b)(2)(iv) | N/A | N/A | The probability and criticality of potential risks to electronic protected health information. | Functional | Intersects With | Risk Framing | RSK-01.1 | Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk. | 5 | |
| § 164.306(b)(2)(iv) | N/A | N/A | The probability and criticality of potential risks to electronic protected health information. | Functional | Intersects With | Risk-Based Security Categorization | RSK-02 | Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that: (1) Document the security categorization results (including supporting rationale) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner. | 5 | |
| § 164.306(b)(2)(iv) | N/A | N/A | The probability and criticality of potential risks to electronic protected health information. | Functional | Intersects With | Risk Identification | RSK-03 | Mechanisms exist to identify and document risks, both internal and external. | 5 | |
| § 164.306(b)(2)(iv) | N/A | N/A | The probability and criticality of potential risks to electronic protected health information. | Functional | Intersects With | Risk Catalog | RSK-03.1 | Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use. | 5 | |
| § 164.306(b)(2)(iv) | N/A | N/A | The probability and criticality of potential risks to electronic protected health information. | Functional | Intersects With | Risk Assessment | RSK-04 | Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD). | 5 | |
| § 164.306(b)(2)(iv) | N/A | N/A | The probability and criticality of potential risks to electronic protected health information. | Functional | Intersects With | Threat Catalog | THR-09 | Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade. | 5 | |
| § 164.306(b)(2)(iv) | N/A | N/A | The probability and criticality of potential risks to electronic protected health information. | Functional | Intersects With | Threat Analysis | THR-10 | Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats. | 5 | |
| § 164.306(c) | N/A | Standards | A covered entity or business associate must comply with the applicable standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314 and § 164.316 with respect to all electronic protected health information. | Functional | Subset Of | Statutory, Regulatory & Contractual Compliance | CPL-01 | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. | 10 | |
| § 164.306(d) | N/A | Implementation specifications | In this subpart: | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.306(d)(1) | N/A | N/A | Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification. | Functional | Subset Of | Statutory, Regulatory & Contractual Compliance | CPL-01 | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. | 10 | |

| HIPAA-HITECH FDE # | NIST SP 800-60 R2 | HIPAA-HITECH FDE Name | HIPAA-HITECH Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship (optional) | Notes (optional) |
|---------------------------|-------------------|--|--|----------------|-------------------|---|----------|---|-------------------------------------|------------------|
| § 164.306(j)(2) | N/A | N/A | When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity or business associate must implement the implementation specifications. | Functional | Subset Of | Statutory, Regulatory & Contractual Compliance | CPL-01 | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. | 10 | |
| § 164.306(j)(3) | N/A | N/A | When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity or business associate must— | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.306(d)(3)(i) | N/A | N/A | Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and | Functional | Intersects With | Cybersecurity & Data Protection Controls Oversight | CPL-02 | Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership. | 5 | |
| § 164.306(d)(3)(ii) | N/A | N/A | Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and | Functional | Intersects With | Cybersecurity & Data Protection Assessments | CPL-03 | Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements. | 5 | |
| § 164.306(d)(3)(iii) | N/A | N/A | Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and | Functional | Intersects With | Functional Review Of Cybersecurity & Data Protection Controls | CPL-03.2 | Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity and data protection policies and standards. | 5 | |
| § 164.306(d)(3)(iv) | N/A | N/A | As applicable to the covered entity or business associate— | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.306(d)(3)(iv)(A) | N/A | N/A | Implement the implementation specification if reasonable and appropriate; or | Functional | Subset Of | Implement Controls | GOV-15.2 | Mechanisms exist to compel data and/or process owners to implement required cybersecurity and data protection controls for each Technology Asset, Application and/or Service (TAAS) under their control. | 10 | |
| § 164.306(d)(3)(iv)(B) | N/A | N/A | If implementing the implementation specification is not reasonable and appropriate— | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.306(d)(3)(iv)(B)(i) | N/A | N/A | Document why it would not be reasonable and appropriate to implement the implementation specification; and | Functional | Subset Of | Exception Management | GOV-02.1 | Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded. | 10 | |
| § 164.306(d)(3)(iv)(B)(2) | N/A | N/A | Implement an equivalent alternative measure if reasonable and appropriate. | Functional | Equal | Compensating Countermeasures | RSK-06.2 | Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats. | 10 | |
| § 164.306(e) | N/A | Maintenance | A covered entity or business associate must review and modify the security measures implemented under this subpart as needed to continue provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measures in accordance with § 164.316(b)(2)(iii). | Functional | Equal | Functional Review Of Cybersecurity & Data Protection Controls | CPL-03.2 | Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity and data protection policies and standards. | 10 | |
| § 164.308 | 164.308 | Administrative safeguards | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.308(a) | N/A | N/A | A covered entity or business associate must, in accordance with § 164.308: | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.308(a)(1) | 164.308(a)(1) | N/A | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.308(a)(1)(i) | 164.308(a)(1) | Standard: Security management process | Implement policies and procedures to prevent, detect, contain, and correct security violations. | Functional | Subset Of | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 10 | |
| § 164.308(a)(1)(i) | 164.308(a)(1) | Standard: Security management process | Implement policies and procedures to prevent, detect, contain, and correct security violations. | Functional | Subset Of | Configuration Management Program | CFG-01 | Mechanisms exist to facilitate the implementation of configuration management controls. | 10 | |
| § 164.308(a)(1)(i) | 164.308(a)(1) | Standard: Security management process | Implement policies and procedures to prevent, detect, contain, and correct security violations. | Functional | Subset Of | Change Management Program | CHG-01 | Mechanisms exist to facilitate the implementation of a change management program. | 10 | |
| § 164.308(a)(1)(i) | 164.308(a)(1) | Standard: Security management process | Implement policies and procedures to prevent, detect, contain, and correct security violations. | Functional | Subset Of | Continuous Monitoring | MON-01 | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls. | 10 | |
| § 164.308(a)(1)(i) | 164.308(a)(1) | Standard: Security management process | Implement policies and procedures to prevent, detect, contain, and correct security violations. | Functional | Subset Of | Incident Response Operations | IRO-01 | Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents. | 10 | |
| § 164.308(a)(1)(ii) | 164.308(a)(1) | Implementation specifications: | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.308(a)(1)(ii)(A) | 164.308(a)(1) | Risk analysis (Required) | Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate. | Functional | Equal | Risk Assessment | RSK-04 | Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD). | 10 | |
| § 164.308(a)(1)(ii)(B) | 164.308(a)(1) | Risk management (Required) | Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a). | Functional | Intersects With | Define Control Objectives | GOV-09 | Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system. | 5 | |
| § 164.308(a)(1)(ii)(B) | 164.308(a)(1) | Risk management (Required) | Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a). | Functional | Subset Of | Implement Controls | GOV-15.2 | Mechanisms exist to compel data and/or process owners to implement required cybersecurity and data protection controls for each Technology Asset, Application and/or Service (TAAS) under their control. | 10 | |
| § 164.308(a)(1)(ii)(C) | 164.308(a)(1) | Sanction policy (Required) | Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate. | Functional | Equal | Personnel Sanctions | HRS-07 | Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures. | 10 | |
| § 164.308(a)(1)(ii)(D) | 164.308(a)(1) | Information system activity review (Required) | Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | Functional | Subset Of | Continuous Monitoring | MON-01 | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls. | 10 | |
| § 164.308(a)(1)(ii)(D) | 164.308(a)(1) | Information system activity review (Required) | Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | Functional | Intersects With | Security Event Monitoring | MON-01.8 | Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures. | 5 | |
| § 164.308(a)(1)(ii)(D) | 164.308(a)(1) | Information system activity review (Required) | Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | Functional | Intersects With | Situational Awareness For Incidents | IRO-09 | Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident. | 5 | |
| § 164.308(a)(2) | 164.308(a)(2) | Standard: Assigned security responsibility | Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate. | Functional | Equal | Assigned Cybersecurity & Data Protection Responsibilities | GOV-04 | Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and data protection program. | 10 | |
| § 164.308(a)(3) | 164.308(a)(3) | N/A | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.308(a)(3)(i) | 164.308(a)(3) | Standard: Workforce security | Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | Functional | Subset Of | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 10 | |
| § 164.308(a)(3)(i) | 164.308(a)(3) | Standard: Workforce security | Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | Functional | Intersects With | Sensitive / Regulated Data Access Enforcement | CFG-08 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to restrict access to sensitive/regulated data. | 5 | |
| § 164.308(a)(3)(i) | 164.308(a)(3) | Standard: Workforce security | Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | Functional | Subset Of | Identity & Access Management (IAM) | IAC-01 | Mechanisms exist to facilitate the implementation of identification and access management controls. | 10 | |
| § 164.308(a)(3)(i) | 164.308(a)(3) | Standard: Workforce security | Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | Functional | Intersects With | Role-Based Access Control (RBAC) | IAC-08 | Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs. | 5 | |
| § 164.308(a)(3)(i) | 164.308(a)(3) | Standard: Workforce security | Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | Functional | Intersects With | Least Privilege | IAC-21 | Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions. | 5 | |
| § 164.308(a)(3)(ii) | 164.308(a)(3) | Implementation specifications: | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.308(a)(3)(ii)(A) | 164.308(a)(3) | Authorization and/or supervision (Addressable) | Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | Functional | Subset Of | Human Resources Security Management | HRS-01 | Mechanisms exist to facilitate the implementation of personnel security controls. | 10 | |
| § 164.308(a)(3)(ii)(A) | 164.308(a)(3) | Authorization and/or supervision (Addressable) | Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | Functional | Intersects With | Change of Roles & Duties | IAC-07.1 | Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted. | 3 | |
| § 164.308(a)(3)(ii)(A) | 164.308(a)(3) | Authorization and/or supervision (Addressable) | Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | Functional | Intersects With | Role-Based Access Control (RBAC) | IAC-08 | Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs. | 5 | |
| § 164.308(a)(3)(ii)(A) | 164.308(a)(3) | Authorization and/or supervision (Addressable) | Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | Functional | Intersects With | Management Approval For New or Changed Accounts | IAC-28.1 | Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts. | 5 | |

| HIPAA-HITECH FDE # | NIST SP 800-66 R2 | HIPAA-HITECH FDE Name | HIPAA-HITECH Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship (optional) | Notes (optional) |
|-----------------------|-------------------|--|---|----------------|-------------------|--|----------|---|-------------------------------------|------------------|
| § 164.308(a)(3)(i)(B) | 164.308(a)(3) | Workforce clearance procedure (Addressable) | Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | Functional | Intersects With | Position Categorization | HRS-02 | Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions. | 5 | |
| § 164.308(a)(3)(i)(B) | 164.308(a)(3) | Workforce clearance procedure (Addressable) | Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | Functional | Intersects With | Defined Roles & Responsibilities | HRS-03 | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel. | 5 | |
| § 164.308(a)(3)(i)(B) | 164.308(a)(3) | Workforce clearance procedure (Addressable) | Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | Functional | Intersects With | Periodic Review of Account Privileges | IAC-17 | Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary. | 5 | |
| § 164.308(a)(3)(i)(C) | 164.308(a)(3) | Termination procedures (Addressable) | Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(i)(B) of this section. | Functional | Intersects With | Personnel Transfer | HRS-08 | Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner. | 5 | |
| § 164.308(a)(3)(i)(C) | 164.308(a)(3) | Termination procedures (Addressable) | Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(i)(B) of this section. | Functional | Intersects With | Personnel Termination | HRS-09 | Mechanisms exist to govern the termination of individual employment. | 5 | |
| § 164.308(a)(3)(i)(C) | 164.308(a)(3) | Termination procedures (Addressable) | Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(i)(B) of this section. | Functional | Intersects With | User Provisioning & De-Provisioning | IAC-07 | Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights. | 5 | |
| § 164.308(a)(3)(i)(C) | 164.308(a)(3) | Termination procedures (Addressable) | Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(i)(B) of this section. | Functional | Intersects With | Termination of Employment | IAC-07.2 | Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract. | 5 | |
| § 164.308(a)(4) | 164.308(a)(4) | N/A | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.308(a)(4)(i) | 164.308(a)(4) | Standard: Information access management | Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part. | Functional | Subset Of | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 10 | |
| § 164.308(a)(4)(i) | 164.308(a)(4) | Standard: Information access management | Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part. | Functional | Subset Of | Identity & Access Management (IAM) | IAC-01 | Mechanisms exist to facilitate the implementation of identification and access management controls. | 10 | |
| § 164.308(a)(4)(ii) | 164.308(a)(4) | Implementation specifications: | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.308(a)(4)(i)(A) | 164.308(a)(4) | Isolating health care clearinghouse functions (Required) | If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | Functional | Subset Of | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 10 | |
| § 164.308(a)(4)(i)(B) | 164.308(a)(4) | Access authorization (Addressable) | Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | Functional | Subset Of | Identity & Access Management (IAM) | IAC-01 | Mechanisms exist to facilitate the implementation of identification and access management controls. | 10 | |
| § 164.308(a)(4)(i)(C) | 164.308(a)(4) | Access establishment and modification (Addressable) | Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | Functional | Equal | Role-Based Access Control (RBAC) | IAC-08 | Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs. | 10 | |
| § 164.308(a)(5) | 164.308(a)(5) | N/A | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.308(a)(5)(i) | 164.308(a)(5) | Standard: Security awareness and training | Implement a security awareness and training program for all members of its workforce (including management). | Functional | Subset Of | Cybersecurity & Data Protection-Minded Workforce | SAT-01 | Mechanisms exist to facilitate the implementation of security workforce development and awareness controls. | 10 | |
| § 164.308(a)(5)(i) | 164.308(a)(5) | Standard: Security awareness and training | Implement a security awareness and training program for all members of its workforce (including management). | Functional | Intersects With | Cybersecurity & Data Protection Awareness Training | SAT-02 | Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function. | 5 | |
| § 164.308(a)(5)(ii) | 164.308(a)(5) | Implementation specifications: | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.308(a)(5)(i)(A) | 164.308(a)(5) | Security reminders (Addressable) | Periodic security updates. | Functional | Equal | Cyber Threat Environment | SAT-03.6 | Mechanisms exist to provide role-based cybersecurity and data protection awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations. | 10 | |
| § 164.308(a)(5)(i)(B) | 164.308(a)(5) | Protection from malicious software (Addressable) | Procedures for guarding against, detecting, and reporting malicious software. | Functional | Equal | Suspicious Communications & Anomalous System Behavior | SAT-03.2 | Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior. | 10 | |
| § 164.308(a)(5)(i)(C) | 164.308(a)(5) | Log-in monitoring (Addressable) | Procedures for monitoring log-in attempts and reporting discrepancies. | Functional | Equal | Role-Based Cybersecurity & Data Protection Training | SAT-03 | Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter. | 10 | |
| § 164.308(a)(5)(i)(D) | 164.308(a)(5) | Password management (Addressable) | Procedures for creating, changing, and safeguarding passwords. | Functional | Equal | Role-Based Cybersecurity & Data Protection Training | SAT-03 | Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter. | 10 | |
| § 164.308(a)(6) | 164.308(a)(6) | N/A | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.308(a)(6)(i) | 164.308(a)(6) | Standard: Security incident procedures | Implement policies and procedures to address security incidents. | Functional | Subset Of | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 10 | |
| § 164.308(a)(6)(i) | 164.308(a)(6) | Standard: Security incident procedures | Implement policies and procedures to address security incidents. | Functional | Subset Of | Incident Response Operations | IRO-01 | Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents. | 10 | |
| § 164.308(a)(6)(ii) | 164.308(a)(6) | Implementation specifications: Response and reporting (Required) | Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. | Functional | Equal | Incident Handling | IRO-02 | Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery. | 10 | |
| § 164.308(a)(7) | 164.308(a)(7) | N/A | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.308(a)(7)(i) | 164.308(a)(7) | Standard: Contingency plan | Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. | Functional | Subset Of | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 10 | |
| § 164.308(a)(7)(i) | 164.308(a)(7) | Standard: Contingency plan | Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. | Functional | Subset Of | Business Continuity Management System (BCMS) | BCD-01 | Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) [e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks]. | 10 | |
| § 164.308(a)(7)(i) | 164.308(a)(7) | Standard: Contingency plan | Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. | Functional | Subset Of | Incident Response Operations | IRO-01 | Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents. | 10 | |
| § 164.308(a)(7)(ii) | 164.308(a)(7) | Implementation specifications: | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.308(a)(7)(i)(A) | 164.308(a)(7) | Data backup plan (Required) | Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | Functional | Equal | Data Backups | BCD-11 | Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). | 10 | |
| § 164.308(a)(7)(i)(B) | 164.308(a)(7) | Disaster recovery plan (Required) | Establish (and implement as needed) procedures to restore any loss of data. | Functional | Equal | Information System Recovery & Reconstitution | BCD-12 | Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure. | 10 | |
| § 164.308(a)(7)(i)(C) | 164.308(a)(7) | Emergency mode operation plan (Required) | Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | Functional | Subset Of | Business Continuity Management System (BCMS) | BCD-01 | Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) [e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks]. | 10 | |
| § 164.308(a)(7)(i)(C) | 164.308(a)(7) | Emergency mode operation plan (Required) | Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | Functional | Intersects With | Continuous Essential Mission & Business Functions | BCD-02.2 | Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration at primary processing and/or storage sites. | 5 | |
| § 164.308(a)(7)(i)(D) | 164.308(a)(7) | Testing and revision procedures (Addressable) | Implement procedures for periodic testing and revision of contingency plans. | Functional | Intersects With | Contingency Plan Testing & Exercises | BCD-04 | Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan. | 5 | |
| § 164.308(a)(7)(i)(D) | 164.308(a)(7) | Testing and revision procedures (Addressable) | Implement procedures for periodic testing and revision of contingency plans. | Functional | Intersects With | Contingency Plan Root Cause Analysis (RCA) & Lessons Learned | BCD-05 | Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated. | 5 | |

| HIPAA-HITECH FDE # | NIST SP 800-66 R2 | HIPAA-HITECH FDE Name | HIPAA-HITECH Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship (optional) | Notes (optional) |
|------------------------|-------------------|---|---|-------------------|----------------------|--|----------|---|---|------------------|
| § 164.308(a)(7)(ii)(E) | 164.308(a)(7) | Applications and data criticality analysis (Addressable) | Assess the relative criticality of specific applications and data in support of other contingency plan components. | Functional | Subset Of | Asset Governance | AST-01 | Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls. | 10 | |
| § 164.308(a)(7)(ii)(E) | 164.308(a)(7) | Applications and data criticality analysis (Addressable) | Assess the relative criticality of specific applications and data in support of other contingency plan components. | Functional | Intersects With | Asset-Service Dependencies | AST-01.1 | Mechanisms exist to identify and assess the security of technology assets that support more than one critical business function. | 8 | |
| § 164.308(a)(7)(ii)(E) | 164.308(a)(7) | Applications and data criticality analysis (Addressable) | Assess the relative criticality of specific applications and data in support of other contingency plan components. | Functional | Intersects With | Identify Critical Assets | BCD-02 | Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions. | 8 | |
| § 164.308(a)(7)(ii)(E) | 164.308(a)(7) | Applications and data criticality analysis (Addressable) | Assess the relative criticality of specific applications and data in support of other contingency plan components. | Functional | Intersects With | Third-Party Criticality Assessments | TPM-02 | Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services. | 3 | |
| § 164.308(a)(8) | 164.308(a)(8) | Standard: Evaluation | Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart. | Functional | Intersects With | Functional Review Of Cybersecurity & Data Protection Controls | CPL-03.2 | Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity and data protection policies and standards. | 5 | |
| § 164.308(a)(8) | 164.308(a)(8) | Standard: Evaluation | Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart. | Functional | Intersects With | Assessment Boundaries | IAO-01.1 | Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review. | 5 | |
| § 164.308(a)(8) | 164.308(a)(8) | Standard: Evaluation | Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart. | Functional | Intersects With | Assessments | IAO-02 | Mechanisms exist to formally assess the cybersecurity and data protection controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements. | 3 | |
| § 164.308(b) | N/A | Business associate contracts and other arrangements | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.308(b)(1) | 164.308(b)(1) | N/A | A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor. | Functional | Subset Of | Third-Party Management | TPM-01 | Mechanisms exist to facilitate the implementation of third-party management controls. | 10 | |
| § 164.308(b)(1) | 164.308(b)(1) | N/A | A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor. | Functional | Intersects With | Third-Party Services | TPM-04 | Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD). | 5 | |
| § 164.308(b)(1) | 164.308(b)(1) | N/A | A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor. | Functional | Intersects With | Third-Party Contract Requirements | TPM-05 | Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD). | 5 | |
| § 164.308(b)(1) | 164.308(b)(1) | N/A | A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor. | Functional | Intersects With | Contract Flow-Down Requirements | TPM-05.2 | Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers. | 5 | |
| § 164.308(b)(1) | 164.308(b)(1) | N/A | A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor. | Functional | Intersects With | Responsible, Accountable, Supportive, Consulted & Informed (RASC) Matrix | TPM-05.4 | Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASC) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs). | 5 | |
| § 164.308(b)(2) | N/A | N/A | A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information. | Functional | Intersects With | Third-Party Contract Requirements | TPM-05 | Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD). | 5 | |
| § 164.308(b)(2) | N/A | N/A | A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information. | Functional | Intersects With | Contract Flow-Down Requirements | TPM-05.2 | Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers. | 5 | |
| § 164.308(b)(2) | N/A | N/A | A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information. | Functional | Intersects With | First-Party Declaration (1PD) | TPM-05.6 | Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity and data protection controls, including any flow-down requirements to subcontractors. | 5 | |
| § 164.308(b)(3) | N/A | Implementation specifications: Written contract or other arrangement (Required) | Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a). | Functional | Intersects With | Adequate Security for Sensitive / Regulated Data In Support of Contracts | IAO-03.2 | Mechanisms exist to protect sensitive / regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract. | 5 | |
| § 164.308(b)(3) | N/A | Implementation specifications: Written contract or other arrangement (Required) | Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a). | Functional | Equal | Third-Party Contract Requirements | TPM-05 | Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD). | 10 | |
| § 164.310 | 164.310 | Physical safeguards | A covered entity or business associate must, in accordance with § 164.309, [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.310(a) | 164.310(a) | N/A | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.310(a)(1) | 164.310(a) | Standard: Facility access controls | Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. | Functional | Subset Of | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 10 | |
| § 164.310(a)(1) | 164.310(a) | Standard: Facility access controls | Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. | Functional | Subset Of | Physical & Environmental Protections | PES-01 | Mechanisms exist to facilitate the operation of physical and environmental protection controls. | 10 | |
| § 164.310(a)(2) | 164.310(a) | Implementation specifications: [no content] | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.310(a)(2)(i) | 164.310(a) | Contingency operations (Addressable) | Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. | Functional | Intersects With | Accessability | BCD-09.2 | Mechanisms exist to identify and mitigate potential accessibility problems to the alternate processing site and possible mitigation actions, in the event of an area-wide disruption or disaster. | 8 | |
| § 164.310(a)(2)(i) | 164.310(a) | Contingency operations (Addressable) | Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. | Functional | Intersects With | Defined Roles & Responsibilities | HRS-03 | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel. | 5 | |
| § 164.310(a)(2)(i) | 164.310(a) | Contingency operations (Addressable) | Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. | Functional | Intersects With | Physical Access Authorizations | PES-02 | Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible). | 5 | |

| HIPAA-HITECH FDE # | NIST SP 800-66 R2 | HIPAA-HITECH FDE Name | HIPAA-HITECH Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship (optional) | Notes (optional) |
|----------------------|-------------------|--|--|----------------|-------------------|--|----------|--|-------------------------------------|------------------|
| § 164.310(a)(2)(ii) | 164.310(a) | Contingency operations (Addressable) | Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. | Functional | Intersects With | Role-Based Physical Access | PES-02.1 | Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual. | 5 | |
| § 164.310(a)(2)(ii) | 164.310(a) | Facility security plan (Addressable) | Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. | Functional | Subset Of | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 10 | |
| § 164.310(a)(2)(ii) | 164.310(a) | Facility security plan (Addressable) | Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. | Functional | Subset Of | Physical & Environmental Protections | PES-01 | Mechanisms exist to facilitate the operation of physical and environmental protection controls. | 10 | |
| § 164.310(a)(2)(ii) | 164.310(a) | Facility security plan (Addressable) | Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. | Functional | Intersects With | Physical Access Control | PES-03 | Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible). | 5 | |
| § 164.310(a)(2)(iii) | 164.310(a) | Access control and validation procedures (Addressable) | Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. | Functional | Subset Of | Identity & Access Management (IAM) | IAC-01 | Mechanisms exist to facilitate the implementation of identification and access management controls. | 10 | |
| § 164.310(a)(2)(iii) | 164.310(a) | Access control and validation procedures (Addressable) | Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. | Functional | Intersects With | Physical Access Authorizations | PES-02 | Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible). | 5 | |
| § 164.310(a)(2)(iii) | 164.310(a) | Access control and validation procedures (Addressable) | Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. | Functional | Intersects With | Physical Access Control | PES-03 | Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible). | 5 | |
| § 164.310(a)(2)(iii) | 164.310(a) | Access control and validation procedures (Addressable) | Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. | Functional | Intersects With | Visitor Control | PES-06 | Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible). | 5 | |
| § 164.310(a)(2)(iv) | 164.310(a) | Maintenance records (Addressable) | Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). | Functional | Subset Of | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 10 | |
| § 164.310(a)(2)(iv) | 164.310(a) | Maintenance records (Addressable) | Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). | Functional | Subset Of | Maintenance Operations | MNT-01 | Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise. | 10 | |
| § 164.310(a)(2)(iv) | 164.310(a) | Maintenance records (Addressable) | Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). | Functional | Intersects With | Controlled Maintenance | MNT-02 | Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the system, application or service. | 8 | |
| § 164.310(a)(2)(iv) | 164.310(a) | Maintenance records (Addressable) | Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). | Functional | Subset Of | Physical & Environmental Protections | PES-01 | Mechanisms exist to facilitate the operation of physical and environmental protection controls. | 10 | |
| § 164.310(b) | 164.310(b) | Standard: Workstation use | Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. | Functional | Subset Of | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 10 | |
| § 164.310(b) | 164.310(b) | Standard: Workstation use | Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. | Functional | Subset Of | Enterprise Device Management (EDM) | END-01 | Mechanisms exist to facilitate the implementation of Enterprise Device Management (EDM) controls. | 10 | |
| § 164.310(b) | 164.310(b) | Standard: Workstation use | Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. | Functional | Intersects With | Terms of Employment | HRS-05 | Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work. | 5 | |
| § 164.310(b) | 164.310(b) | Standard: Workstation use | Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. | Functional | Intersects With | Rules of Behavior | HRS-05.1 | Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior. | 3 | |
| § 164.310(b) | 164.310(b) | Standard: Workstation use | Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. | Functional | Intersects With | Use of Communications Technology | HRS-05.3 | Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously. | 3 | |
| § 164.310(b) | 164.310(b) | Standard: Workstation use | Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. | Functional | Intersects With | Standardized Operating Procedures (SOP) | OPS-01.1 | Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks. | 5 | |
| § 164.310(b) | 164.310(b) | Standard: Workstation use | Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. | Functional | Intersects With | Service Delivery (Business Process Support) | OPS-03 | Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area. | 3 | |
| § 164.310(b) | 164.310(b) | Standard: Workstation use | Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. | Functional | Intersects With | Access To Information Systems | PES-03.4 | Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulatory data, in addition to the physical access controls for the facility. | 3 | |
| § 164.310(b) | 164.310(b) | Standard: Workstation use | Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. | Functional | Intersects With | Physical Security of Offices, Rooms & Facilities | PES-04 | Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities. | 3 | |
| § 164.310(c) | 164.310(c) | Standard: Workstation security | Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users. | Functional | Subset Of | Endpoint Protection Measures | END-02 | Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices. | 10 | |
| § 164.310(c) | 164.310(c) | Standard: Workstation security | Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users. | Functional | Intersects With | Physical Access Control | PES-03 | Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible). | 5 | |
| § 164.310(c) | 164.310(c) | Standard: Workstation security | Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users. | Functional | Intersects With | Access To Information Systems | PES-03.4 | Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulatory data, in addition to the physical access controls for the facility. | 5 | |
| § 164.310(c) | 164.310(c) | Standard: Workstation security | Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users. | Functional | Intersects With | Physical Security of Offices, Rooms & Facilities | PES-04 | Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities. | 5 | |
| § 164.310(c) | 164.310(c) | Standard: Workstation security | Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users. | Functional | Intersects With | Working in Secure Areas | PES-04.1 | Physical security mechanisms exist to allow only authorized personnel access to secure areas. | 5 | |
| § 164.310(d) | 164.310(d) | Standard: Device and media controls | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.310(d)(1) | 164.310(d) | N/A | Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. | Functional | Subset Of | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 10 | |
| § 164.310(d)(1) | 164.310(d) | N/A | Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. | Functional | Subset Of | Asset Governance | AST-01 | Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls. | 10 | |
| § 164.310(d)(1) | 164.310(d) | N/A | Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. | Functional | Intersects With | Removal of Assets | AST-11 | Mechanisms exist to authorize, control and track technology assets entering and exiting organizational facilities. | 5 | |
| § 164.310(d)(1) | 164.310(d) | N/A | Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. | Functional | Subset Of | Data Protection | DCH-01 | Mechanisms exist to facilitate the implementation of data protection controls. | 10 | |
| § 164.310(d)(1) | 164.310(d) | N/A | Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. | Functional | Intersects With | Media Access | DCH-03 | Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals. | 5 | |

| HIPAA-HITECH FDE # | NIST SP 800-66 R2 | HIPAA-HITECH FDE Name | HIPAA-HITECH Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship (optional) | Notes (optional) |
|----------------------|-------------------|---|---|----------------|-------------------|--|-----------|---|-------------------------------------|------------------|
| § 164.310(d)(1) | 164.310(d) | N/A | Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. | Functional | Intersects With | Media Transportation | DCH-07 | Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures. | 5 | |
| § 164.310(d)(1) | 164.310(d) | N/A | Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. | Functional | Intersects With | Custodians | DCH-07.1 | Mechanisms exist to identify custodians throughout the transport of digital or non-digital media. | 5 | |
| § 164.310(d)(1) | 164.310(d) | N/A | Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. | Functional | Intersects With | Portable Storage Devices | DCH-13.2 | Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems. | 5 | |
| § 164.310(d)(1) | 164.310(d) | N/A | Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. | Functional | Subset Of | Maintenance Operations | MNT-01 | Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise. | 10 | |
| § 164.310(d)(1) | 164.310(d) | N/A | Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. | Functional | Intersects With | Prevent Unauthorized Removal | MNT-04.3 | Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that containing organizational information. | 5 | |
| § 164.310(d)(2) | 164.310(d) | Implementation specifications: | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.310(d)(2)(i) | 164.310(d) | Disposal (Required) | Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored. | Functional | Subset Of | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 10 | |
| § 164.310(d)(2)(i) | 164.310(d) | Disposal (Required) | Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored. | Functional | Subset Of | Asset Governance | AST-01 | Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls. | 10 | |
| § 164.310(d)(2)(i) | 164.310(d) | Disposal (Required) | Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored. | Functional | Intersects With | Secure Disposal, Destruction or Re-Use of Equipment | AST-09 | Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components. | 5 | |
| § 164.310(d)(2)(ii) | 164.310(d) | Media re-use (Required) | Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use. | Functional | Intersects With | Secure Disposal, Destruction or Re-Use of Equipment | AST-09 | Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components. | 5 | |
| § 164.310(d)(2)(ii) | 164.310(d) | Media re-use (Required) | Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use. | Functional | Intersects With | System Media Sanitization | DCH-09 | Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse. | 5 | |
| § 164.310(d)(2)(iii) | 164.310(d) | Accountability (Addressable) | Maintain a record of the movements of hardware and electronic media and any person responsible therefore. | Functional | Intersects With | Asset Inventories | AST-02 | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel. | 3 | |
| § 164.310(d)(2)(iii) | 164.310(d) | Accountability (Addressable) | Maintain a record of the movements of hardware and electronic media and any person responsible therefore. | Functional | Intersects With | Updates During Installations / Removals | AST-02.1 | Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades. | 3 | |
| § 164.310(d)(2)(iii) | 164.310(d) | Accountability (Addressable) | Maintain a record of the movements of hardware and electronic media and any person responsible therefore. | Functional | Intersects With | Configuration Management Database (CMDB) | AST-02.9 | Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information. | 5 | |
| § 164.310(d)(2)(iii) | 164.310(d) | Accountability (Addressable) | Maintain a record of the movements of hardware and electronic media and any person responsible therefore. | Functional | Intersects With | Asset Ownership Assignment | AST-03 | Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection. | 5 | |
| § 164.310(d)(2)(iii) | 164.310(d) | Accountability (Addressable) | Maintain a record of the movements of hardware and electronic media and any person responsible therefore. | Functional | Intersects With | Accountability Information | AST-03.1 | Mechanisms exist to include capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory process. | 5 | |
| § 164.310(d)(2)(iv) | 164.310(d) | Data backup and storage (Addressable) | Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment. | Functional | Intersects With | Data Backups | BCD-11 | Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). | 3 | |
| § 164.312 | 164.312 | Technical safeguards | A covered entity or business associate must, in accordance with § 164.306: | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.312(a) | 164.312(a) | Standard: Access control | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.312(a)(1) | 164.312(a) | N/A | Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.306(a)(4). | Functional | Subset Of | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 10 | |
| § 164.312(a)(1) | 164.312(a) | N/A | Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.306(a)(4). | Functional | Intersects With | Position Categorization | HRS-02 | Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions. | 5 | |
| § 164.312(a)(1) | 164.312(a) | N/A | Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.306(a)(4). | Functional | Intersects With | Defined Roles & Responsibilities | HRS-03 | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel. | 5 | |
| § 164.312(a)(1) | 164.312(a) | N/A | Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.306(a)(4). | Functional | Subset Of | Identity & Access Management (IAM) | IAC-01 | Mechanisms exist to facilitate the implementation of identification and access management controls. | 10 | |
| § 164.312(a)(1) | 164.312(a) | N/A | Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.306(a)(4). | Functional | Intersects With | Role-Based Access Control (RBAC) | IAC-08 | Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs. | 5 | |
| § 164.312(a)(1) | 164.312(a) | N/A | Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.306(a)(4). | Functional | Intersects With | Least Privilege | IAC-21 | Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions. | 5 | |
| § 164.312(a)(2) | 164.312(a) | Implementation specifications: | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.312(a)(2)(i) | 164.312(a) | Unique user identification (Required) | Assign a unique name and/or number for identifying and tracking user identity. | Functional | Subset Of | Identification & Authentication for Organizational Users | IAC-02 | Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users. | 10 | |
| § 164.312(a)(2)(i) | 164.312(a) | Unique user identification (Required) | Assign a unique name and/or number for identifying and tracking user identity. | Functional | Equal | Identifier Management (User Names) | IAC-09 | Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS). | 10 | |
| § 164.312(a)(2)(ii) | 164.312(a) | Emergency access procedure (Required) | Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. | Functional | Subset Of | Account Management | IAC-15 | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts. | 10 | |
| § 164.312(a)(2)(ii) | 164.312(a) | Emergency access procedure (Required) | Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. | Functional | Intersects With | Removal of Temporary / Emergency Accounts | IAC-15.2 | Automated mechanisms exist to disable or remove temporary and emergency accounts after an organization-defined time period for each type of account. | 3 | |
| § 164.312(a)(2)(ii) | 164.312(a) | Emergency access procedure (Required) | Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. | Functional | Equal | Emergency Accounts | IAC-15.9 | Mechanisms exist to establish and control "emergency access only" accounts. | 10 | |
| § 164.312(a)(2)(iii) | 164.312(a) | Automatic logoff (Addressable) | Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. | Functional | Intersects With | System Hardening Through Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | |
| § 164.312(a)(2)(iii) | 164.312(a) | Automatic logoff (Addressable) | Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. | Functional | Intersects With | Session Termination | IAC-25 | Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity. | 5 | |
| § 164.312(a)(2)(iv) | 164.312(a) | Encryption and decryption (Addressable) | Implement a mechanism to encrypt and decrypt electronic protected health information. | Functional | Subset Of | Use of Cryptographic Controls | CRY-01 | Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies. | 10 | |
| § 164.312(b) | 164.312(b) | Standard: Audit controls | Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | Functional | Subset Of | Continuous Monitoring | MON-01 | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls. | 10 | |
| § 164.312(b) | 164.312(b) | Standard: Audit controls | Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | Functional | Intersects With | System Generated Alerts | MON-01.4 | Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness. | 5 | |
| § 164.312(b) | 164.312(b) | Standard: Audit controls | Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | Functional | Intersects With | Security Event Monitoring | MON-01.8 | Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures. | 5 | |
| § 164.312(b) | 164.312(b) | Standard: Audit controls | Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | Functional | Intersects With | Analyze and Prioritize Monitoring Requirements | MON-01.16 | Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of assets, based on asset criticality and the sensitivity of the data it stores, transmits and processes. | 5 | |

| HIPAA-HITECH FDE # | NIST SP 800-66 R2 | HIPAA-HITECH FDE Name | HIPAA-HITECH Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship (optional) | Notes (optional) |
|-----------------------|-------------------|---|--|----------------|-------------------|--|-----------|--|-------------------------------------|------------------|
| § 164.312(b) | 164.312(b) | Standard: Audit controls | Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | Functional | Intersects With | Content of Event Logs | MON-03 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event. | 5 | |
| § 164.312(b) | 164.312(b) | Standard: Audit controls | Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | Functional | Intersects With | Audit Trails | MON-03.2 | Mechanisms exist to link system access to individual users or service accounts. | 5 | |
| § 164.312(b) | 164.312(b) | Standard: Audit controls | Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | Functional | Intersects With | Anomalous Behavior | MON-16 | Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities. | 5 | |
| § 164.312(c) | 164.312(c) | Standard: Integrity | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.312(c)(1) | 164.312(c) | N/A | Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. | Functional | Subset Of | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 10 | |
| § 164.312(c)(1) | 164.312(c) | N/A | Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. | Functional | Subset Of | Data Protection | DCH-01 | Mechanisms exist to facilitate the implementation of data protection controls. | 10 | |
| § 164.312(c)(1) | 164.312(c) | N/A | Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. | Functional | Intersects With | Sensitive / Regulated Data Protection | DCH-01.2 | Mechanisms exist to protect sensitive/regulated data wherever it is stored. | 5 | |
| § 164.312(c)(2) | 164.312(c) | Implementation specification: Mechanism to authenticate electronic protected health information (Addressable) | Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. | Functional | Intersects With | Sensitive / Regulated Data Access Enforcement | CFG-08 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to restrict access to sensitive/regulated data. | 5 | |
| § 164.312(c)(2) | 164.312(c) | Implementation specification: Mechanism to authenticate electronic protected health information (Addressable) | Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. | Functional | Intersects With | Sensitive / Regulated Data Actions | CFG-08.1 | Automated mechanisms exist to generate event logs whenever sensitive/regulated data is collected, created, updated, deleted and/or archived. | 5 | |
| § 164.312(c)(2) | 164.312(c) | Implementation specification: Mechanism to authenticate electronic protected health information (Addressable) | Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. | Functional | Intersects With | File Integrity Monitoring (FIM) | MON-01.7 | Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical assets to generate alerts for unauthorized modifications. | 5 | |
| § 164.312(c)(2) | 164.312(c) | Implementation specification: Mechanism to authenticate electronic protected health information (Addressable) | Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. | Functional | Intersects With | Privileged User Oversight | MON-01.15 | Mechanisms exist to implement enhanced activity monitoring for privileged users. | 5 | |
| § 164.312(c)(2) | 164.312(c) | Implementation specification: Mechanism to authenticate electronic protected health information (Addressable) | Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. | Functional | Intersects With | Anomalous Behavior | MON-16 | Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities. | 5 | |
| § 164.312(d) | 164.312(d) | Standard: Person or entity authentication | Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. | Functional | Subset Of | Human Resources Security Management | HRS-01 | Mechanisms exist to facilitate the implementation of personnel security controls. | 10 | |
| § 164.312(d) | 164.312(d) | Standard: Person or entity authentication | Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. | Functional | Intersects With | Personnel Screening | HRS-04 | Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access. | 5 | |
| § 164.312(d) | 164.312(d) | Standard: Person or entity authentication | Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. | Functional | Intersects With | Identity Proofing (Identity Verification) | IAC-28 | Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions. | 5 | |
| § 164.312(d) | 164.312(d) | Standard: Person or entity authentication | Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. | Functional | Intersects With | Identity Evidence | IAC-28.2 | Mechanisms exist to require evidence of individual identification to be presented to the registration authority. | 5 | |
| § 164.312(d) | 164.312(d) | Standard: Person or entity authentication | Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. | Functional | Intersects With | Identity Evidence Validation & Verification | IAC-28.3 | Mechanisms exist to require that the presented identity evidence be validated and verified through organizational-defined methods of validation and verification. | 5 | |
| § 164.312(d) | 164.312(d) | Standard: Person or entity authentication | Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. | Functional | Subset Of | Third-Party Management | TPM-01 | Mechanisms exist to facilitate the implementation of third-party management controls. | 10 | |
| § 164.312(e) | N/A | Standard: Transmission security | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.312(e)(1) | 164.312(e)(1) | N/A | Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | Functional | Intersects With | System Hardening Through Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | |
| § 164.312(e)(1) | 164.312(e)(1) | N/A | Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | Functional | Intersects With | Transmission Confidentiality | CRY-03 | Cryptographic mechanisms exist to protect the confidentiality of data being transmitted. | 5 | |
| § 164.312(e)(1) | 164.312(e)(1) | N/A | Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | Functional | Subset Of | Network Security Controls (NSC) | NET-01 | Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC). | 10 | |
| § 164.312(e)(2) | N/A | Implementation specification: | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.312(e)(2)(i) | N/A | Integrity controls (Addressable) | Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | Functional | Intersects With | System Hardening Through Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | |
| § 164.312(e)(2)(i) | N/A | Integrity controls (Addressable) | Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | Functional | Intersects With | Transmission Integrity | CRY-04 | Cryptographic mechanisms exist to protect the integrity of data being transmitted. | 5 | |
| § 164.312(e)(2)(i) | N/A | Integrity controls (Addressable) | Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | Functional | Subset Of | Network Security Controls (NSC) | NET-01 | Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC). | 10 | |
| § 164.312(e)(2)(ii) | N/A | Encryption (Addressable) | Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | Functional | Intersects With | System Hardening Through Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | |
| § 164.312(e)(2)(ii) | N/A | Encryption (Addressable) | Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | Functional | Subset Of | Use of Cryptographic Controls | CRY-01 | Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies. | 10 | |
| § 164.312(e)(2)(ii) | N/A | Encryption (Addressable) | Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | Functional | Intersects With | Service Delivery (Business Process Support) | OPS-03 | Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area. | 5 | |
| § 164.314 | 164.314 | Organizational requirements | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.314(a) | 164.314(a) | N/A | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.314(a)(1) | 164.314(a) | Standard: Business associate contracts or other arrangements | The contract or other arrangement required by § 164.308(b)(3) must meet the requirements of paragraph (a)(2)(ii), (a)(2)(iii), or (a)(2)(iv) of this section, as applicable. | Functional | Subset Of | Statutory, Regulatory & Contractual Compliance | CPL-01 | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. | 10 | |
| § 164.314(a)(2) | 164.314(a) | Implementation specifications (Required) | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.314(a)(2)(i) | 164.314(a) | Business associate contracts | The contract must provide that the business associate will— | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.314(a)(2)(i)(A) | 164.314(a) | N/A | Comply with the applicable requirements of this subpart; | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |

| HIPAA-HITECH FDE # | NIST SP 800-66 R2 | HIPAA-HITECH FDE Name | HIPAA-HITECH Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship (optional) | Notes (optional) |
|-----------------------|-------------------|--|---|-------------------|----------------------|---|----------|--|---|------------------|
| § 164.314(a)(2)(i)(B) | 164.314(a) | N/A | In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section and | Functional | Equal | Contract Flow-Down Requirements | TPM-05.2 | Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers. | 10 | |
| § 164.314(a)(2)(i)(C) | 164.314(a) | N/A | Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410. | Functional | Equal | Security Compromise Notification Agreements | TPM-05.1 | Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes. | 10 | |
| § 164.314(a)(2)(ii) | 164.314(a) | Other arrangements | The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3). | Functional | Subset Of | Statutory, Regulatory & Contractual Compliance | CPL-01 | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. | 10 | |
| § 164.314(a)(2)(iii) | 164.314(a) | Business associate contracts with subcontractors | The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate. | Functional | Intersects With | Third-Party Contract Requirements | TPM-05 | Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD). | 5 | |
| § 164.314(a)(2)(iii) | 164.314(a) | Business associate contracts with subcontractors | The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate. | Functional | Intersects With | Contract Flow-Down Requirements | TPM-05.2 | Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers. | 5 | |
| § 164.314(b) | 164.314(b) | N/A | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.314(b)(1) | 164.314(b) | Standard: Requirements for group health plans | Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(i) or (ii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | Functional | Equal | Third-Party Contract Requirements | TPM-05 | Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD). | 10 | |
| § 164.314(b)(2) | 164.314(b) | Implementation specifications (Required) | The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to— | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.314(b)(2)(i) | 164.314(b) | N/A | Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan. | Functional | Equal | Third-Party Contract Requirements | TPM-05 | Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD). | 10 | |
| § 164.314(b)(2)(ii) | 164.314(b) | N/A | Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; | Functional | Equal | Third-Party Contract Requirements | TPM-05 | Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD). | 10 | |
| § 164.314(b)(2)(iii) | 164.314(b) | N/A | Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and | Functional | Equal | Third-Party Contract Requirements | TPM-05 | Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD). | 10 | |
| § 164.314(b)(2)(iv) | 164.314(b) | N/A | Report to the group health plan any security incident of which it becomes aware. | Functional | Equal | Security Compromise Notification Agreements | TPM-05.1 | Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes. | 10 | |
| § 164.316 | 164.316 | Policies and procedures and documentation requirements | A covered entity or business associate must, in accordance with § 164.306: | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.316(a) | 164.316(a) | Standard: Policies and procedures | Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart. | Functional | Subset Of | Cybersecurity & Data Protection Governance Program | GOV-01 | Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. | 10 | |
| § 164.316(a) | 164.316(a) | Standard: Policies and procedures | Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart. | Functional | Subset Of | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 10 | |
| § 164.316(b) | 164.316(b) | N/A | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.316(b)(1) | 164.316(b) | N/A | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.316(b)(1)(i) | 164.316(b) | Standard: Documentation | Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and | Functional | Subset Of | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 10 | |
| § 164.316(b)(1)(ii) | 164.316(b) | N/A | If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment. | Functional | Intersects With | Periodic Review & Update of Cybersecurity & Data Protection Program | GOV-03 | Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. | 3 | |
| § 164.316(b)(1)(ii) | 164.316(b) | N/A | If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment. | Functional | Intersects With | Cybersecurity & Data Protection Assessments | CPL-03 | Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements. | 3 | |
| § 164.316(b)(2) | 164.316(b) | Implementation specifications: [no content] | [no content] | Functional | No Relationship | N/A | N/A | No applicable SCF control | N/A | |
| § 164.316(b)(2)(i) | 164.316(b) | Time limit (Required) | Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later. | Functional | Equal | Media & Data Retention | DCH-18 | Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations. | 10 | |
| § 164.316(b)(2)(ii) | 164.316(b) | Availability (Required) | Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains. | Functional | Intersects With | Standardized Operating Procedures (SOP) | OPS-01.1 | Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks. | 5 | |
| § 164.316(b)(2)(ii) | 164.316(b) | Availability (Required) | Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains. | Functional | Intersects With | Service Delivery (Business Process Support) | OPS-03 | Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area. | 5 | |
| § 164.316(b)(2)(iii) | 164.316(b) | Updates (Required) | Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information. | Functional | Intersects With | Periodic Review & Update of Cybersecurity & Data Protection Program | GOV-03 | Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. | 5 | |
| § 164.316(b)(2)(iii) | 164.316(b) | Updates (Required) | Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information. | Functional | Intersects With | Cybersecurity & Data Protection Controls Oversight | CPL-02 | Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership. | 5 | |