Claritas Rx Inc.

Type II System and Organization Controls Report (SOC 2)

Report on a Service Organization's Description of Its System and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security and Confidentiality Throughout the Period January 1, 2021, to December 31, 2021.

KirkpatrickPrice
4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

SECTION I: ASSERTION OF CLARITAS RX INC. MANAGEMENT 1

Assertion of Claritas Rx Inc. Management 2

SECTION II: INDEPENDENT SERVICE AUDITOR'S REPORT 4

Independent Service Auditor's Report 5

Scope 5

Service Organization's Responsibilities 6

Service Auditor's Responsibilities 6

Inherent Limitations 7

Description of Tests of Controls 7

Opinion 7

Restricted Use 8

SECTION III: CLARITAS RX INC.'S DESCRIPTION OF ITS DATA AGGREGATION AND PATIENT JOURNEY ANALYTICS SOFTWARE SYSTEM 9

Services Provided 10

Channel Data Strategy 10

Data Aggregation 10

Data Integration 10

Data Analytics 10

Principal Service Commitments and System Requirements 11

Regulatory Commitments 11

Contractual Commitments 11

System Design 11

Components of the System Used to Provide the Services 12

Infrastructure 12

Software 12

People 13

Data 13

Data Confidentiality and Classification 14

Data Encryption 15

Data Retention 15

Processes and Procedures 15

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring 17

Control Environment 17

Management Philosophy 17
Security and Confidentiality Management 17
Security and Confidentiality Policies 17
Personnel Security 18
Physical Security 18
South San Francisco 18
Lexington 19
Media Destruction 19
Change Management 20
Configuration Management 20
Application Development 20
Application Change Management 21
System Monitoring 22
Application Monitoring and Vulnerability Management 22
Problem Management 22
Data Backup and Recovery 23
System Account Management 24
Customer Access 25
Risk Assessment Process 26
Information and Communication Systems 26
Third-Party Breach Reporting 26
Customer Reports and Best Practices Documentation 26
Vendor Management 27
Monitoring Controls 27
Changes to the System During the Period 28
Complementary User-Entity Controls 29
SECTION IV: TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS 31
Applicable Trust Services Criteria Relevant to security and confidentiality 32
Security 32
Confidentiality 32
Trust Services Criteria for the Security and Confidentiality Categories 33
Control Environment 33
Communication and Information 48
Risk Assessment 55
Monitoring Activities 59
Control Activities 62

Logical and Physical Access Controls 71
System Operations 89
Change Management 97
Risk Mitigation 104
Additional Criteria for Confidentiality 110

SECTION I:
ASSERTION OF CLARITAS RX INC. MANAGEMENT

ASSERTION OF CLARITAS RX INC. MANAGEMENT

We have prepared the accompanying description in section III titled "Claritas Rx Inc.'s Description of Its Data Aggregation and Patient Journey Analytics Software System" throughout the period January 1, 2021, to December 31, 2021, (description), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the data aggregation and patient journey analytics software system that may be useful when assessing the risks arising from interactions with Claritas Rx Inc.'s system, particularly information about system controls that Claritas Rx Inc. has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Claritas Rx Inc. uses the following subservice organizations:

- Amazon Web Services for cloud hosting and data storage services
- Box for file storage services
- Quickbase for development software, hosting, customer relationship management (CRM), and accounting services

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Claritas Rx Inc., to achieve Claritas Rx Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Claritas Rx Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Claritas Rx Inc.'s controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Claritas Rx Inc., to achieve Claritas Rx Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Claritas Rx Inc.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Claritas Rx Inc.'s controls.

We confirm, to the best of our knowledge and belief, that

a. the description presents Claritas Rx Inc.'s data aggregation and patient journey analytics software system that was designed and implemented throughout the period January 1, 2021, to December 31, 2021, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period January 1, 2021, to December 31, 2021, to provide reasonable assurance that Claritas Rx Inc.'s service commitments and system requirements would be achieved based on the applicable

trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Claritas Rx Inc.'s controls throughout that period.

c. the controls stated in the description operated effectively throughout the period January 1, 2021, to December 31, 2021, to provide reasonable assurance that Claritas Rx Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Claritas Rx Inc.'s controls operated effectively throughout that period.

SECTION II:
INDEPENDENT SERVICE AUDITOR'S REPORT

Michael Fitzgibbons
Chief Executive Officer & Founder
Claritas Rx Inc.
400 Oyster Point Blvd. #329
South San Francisco, CA 94080

Scope

We have examined Claritas Rx Inc.'s accompanying description in section III titled "Claritas Rx Inc.'s Description of Its Data Aggregation and Patient Journey Analytics Software System" throughout the period January 1, 2021, to December 31, 2021, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2021, to December 31, 2021, to provide reasonable assurance that Claritas Rx Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Due to the global pandemic declared by the World Health Organization on March 11, 2020, physical and environmental controls were tested using virtual and remote video technologies.

Claritas Rx Inc. uses the following subservice organizations:

- Amazon Web Services for cloud hosting and data storage services
- Box for file storage services
- Quickbase for development software, hosting, customer relationship management (CRM), and accounting services

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Claritas Rx Inc., to achieve Claritas Rx Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Claritas Rx Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Claritas Rx Inc.'s controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Claritas Rx Inc., to achieve Claritas Rx Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Claritas Rx Inc.'s controls, the applicable trust services criteria, and the

complementary user entity controls assumed in the design of Claritas Rx Inc.'s controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Claritas Rx Inc. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Claritas Rx Inc.'s service commitments and system requirements were achieved. In section I, Claritas Rx Inc. has provided its assertion titled "Assertion of Claritas Rx Inc. Management" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. Claritas Rx Inc. is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in section IV, "Trust Services Categories, Criteria, Related Controls, and Tests of Controls," of this report in columns 2, 3, and 4, respectively.

Opinion

In our opinion, in all material respects,

a. the description presents Claritas Rx Inc.'s data aggregation and patient journey analytics software system that was designed and implemented throughout the period January 1, 2021, to December 31, 2021, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period January 1, 2021, to December 31, 2021, to provide reasonable assurance that Claritas Rx Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of Claritas Rx Inc.'s controls throughout that period.

c. the controls stated in the description operated effectively throughout the period January 1, 2021, to December 31, 2021, to provide reasonable assurance that Claritas Rx Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Claritas Rx Inc.'s controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section IV, is intended solely for the information and use of Claritas Rx Inc., user entities of Claritas Rx Inc.'s data aggregation and patient journey analytics software system during some or all of the period January 1, 2021, to December 31, 2021, business partners of Claritas Rx Inc. subject to risks arising from interactions with the data aggregation and patient journey analytics software system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

March 14, 2022

SECTION III:
CLARITAS RX INC.'S DESCRIPTION OF ITS DATA AGGREGATION AND PATIENT JOURNEY ANALYTICS SOFTWARE SYSTEM

With locations in South San Francisco, California, and Lexington, Kentucky, Claritas Rx Inc. (Claritas Rx) provides data aggregation and patient journey analytics software-as-a-service (SaaS). The SaaS condenses patient and proprietor communications so manufacturers, providers, and payers can help patients benefit from customers' specialty therapies, such as orphan biopharmaceuticals. Claritas Rx licenses its proprietary platform to its customers to address consuming, analyzing, and using patient-level specialty product data by focusing on patient-level data integration and validation.

The four primary features of the Claritas Rx platform are described in the sections below.

Channel Data Strategy

The channel data strategy considers the nuances and limitations of different data sources to ensure that customers' commercial analytics needs are met. Claritas Rx leverages insights from its data platform to advise customers on best practices in pharmacy network design, use of specialty pharmacy data, and considerations of scaling commercial data infrastructure. The organization's involvement across stages of launch or lifecycle planning helps customers leverage its distribution channels as a competitive advantage.

Data Aggregation

Claritas Rx uses its integrated data dictionary, which is based on experience working with providers and their data, to validate and normalize data. This dictionary equates data elements between providers and allows Claritas Rx to audit the state of customer data at any point and time, allowing customers to focus on bringing specialty medicine to patients.

Data Integration

Claritas Rx uses a data integration process of partner systems and commercial pharmaceutical analytics needs to integrate channel data using algorithms and statistical analyses to yield actionable, patient-level insights.

Data Analytics

The Claritas Rx platform can provide self-service and ad hoc analytics through its business intelligence portal. The organization's custom, role-based applications empower commercial and clinical teams with the data sets they need to make critical, informed decisions.

Regulatory Commitments

Claritas Rx is directly impacted by the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act as it processes, stores, or transmits electronically protected health information (ePHI). These regulatory commitments specifically impact Claritas Rx's data governance program, which is in place to ensure proper security and retention of protected health information (PHI). A HIPAA evaluation is conducted annually to ensure organizational compliance with HIPAA requirements and standards.

Contractual Commitments

Master Service Agreements (MSAs) and/or Statements of Work (SOWs) are agreed upon with customers prior to engaging in any service offering. If service-level agreements (SLAs) are determined, they are agreed upon at a case-base-case basis and tracked by Customer Success, and commitments and SLAs with customers are documented and tracked within customer-specific spreadsheets. Claritas Rx classifies its customer SLA commitments into the following three categories:

1. System up-time commitments
2. Data processing commitments
3. Personnel availability commitments

System Design

Claritas Rx designs its data aggregation and patient journey analytics software system to meet its regulatory and contractual commitments. These commitments are based on the services that Claritas Rx provides to its customers, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that Claritas Rx has established for its services. Claritas Rx establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in Claritas Rx's system policies and procedures, system design documentation, and contracts with customers.

Infrastructure

Claritas Rx's infrastructure is composed of servers, workstations, firewalls, and other networking and telecommunications devices. To illustrate this infrastructure, the organization maintains the Network Connectivity Diagram (below), which illustrates the company's networks, servers, and devices. This diagram is reviewed and updated by the Principal Engineer annually and after any significant changes to the environment.

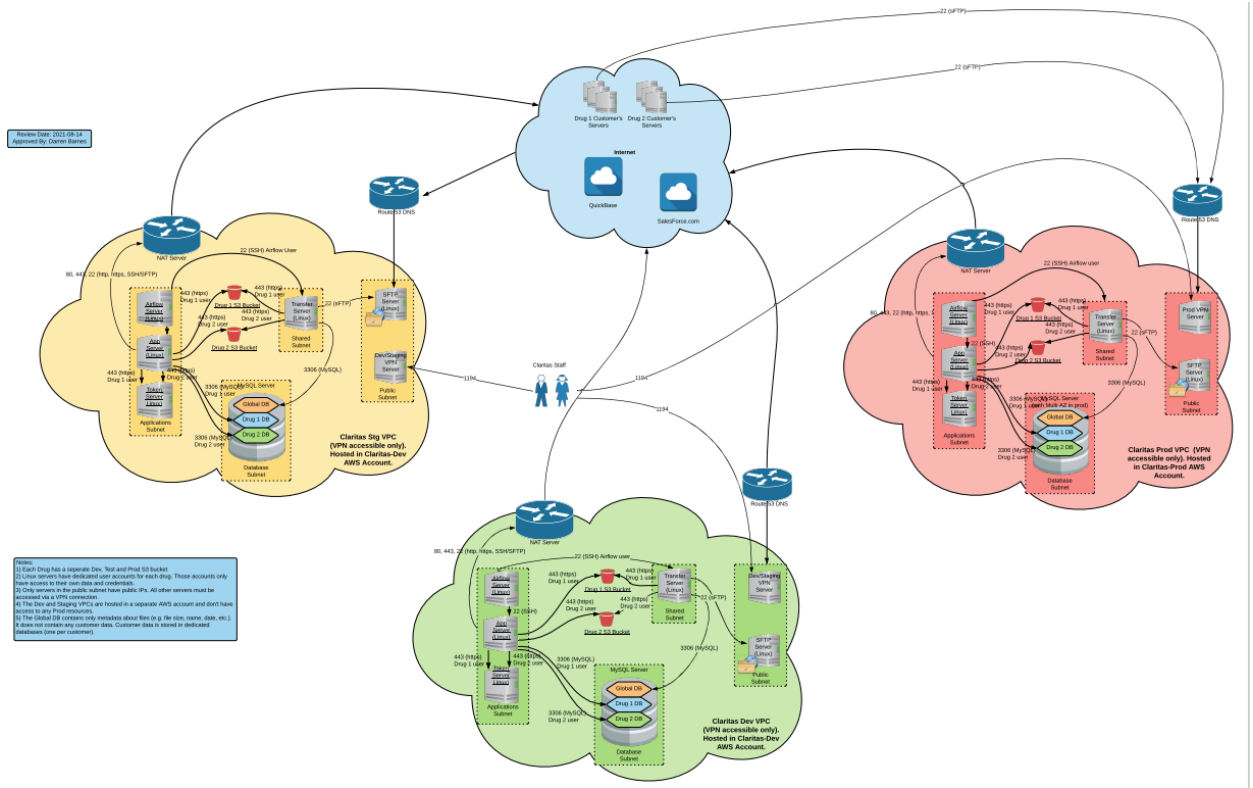

Figure 1: Claritas Rx's Network Connectivity Diagram

All company systems, workstations, devices, and servers are documented and aggregated into a main system inventory that documents the use, function, and location of each item.

Software

A formal software inventory is maintained that documents all of the company's critical software in use, which include the following:

- Airflow
- AlertLogic Forwarder
- Ansible
- Ansible AWX
- CentOS
- Clam AV
- Datavant
- Git
- Gnome Desktop
- Java
- Jupiter
- MS Windows Server
- MySQL Client
- Python
- S3cmd
- Splunk Universal Forwarder
- Tableau Server
- Talend Open Studio
- Unison

People

Oversight of Claritas Rx's governance, strategic direction, and accountability is provided by its Board of Directors, which consists of five members. The Board meets quarterly to review the goals and objectives of the organization.

Claritas Rx's traditional hierarchy, clear reporting lines, and functional departments are illustrated within a formal organizational chart (below). Its functional departments include the following.

- Leadership—the Leadership Team, which reports to the CEO and is responsible for the other functional areas
- Analytics—enables customers to gain insights from integrated self-service data sets
- Corporate Strategy and Business Development—determines the company's goals and business strategy
- Customer Success—represents the needs of the customer
- Delivery & Operations—performs data operations and business analysis
- Engineering—builds solutions based on needs defined by the Implementation and Product Teams
- Finance—performs contract management and compliance
- People Operations—performs Human Resources functions
- Product Management—determines product definitions and oversees product development

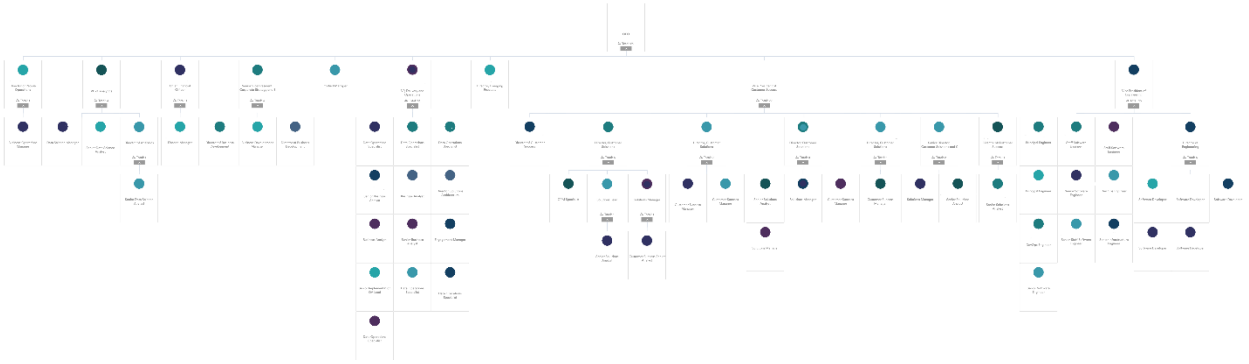

Figure 2: Claritas Rx's organizational chart

Data

Claritas Rx captures utilization data regarding pharmaceutical products from pharmacies and other service providers that support the treatment of patients, including information on patients, transactions such as shipments and benefit verification with patients, data on patient benefits that are provided by their insurers, and prescription information submitted by physicians. The organization also captures information on physical movement of drug products such as shipments and inventory levels, and its proprietary application allows case managers who are working with patients or managing the patient experience to log notes regarding their work or their interactions with patients, healthcare providers, or healthcare payers. All of this information is utilized by pharmaceutical manufactures to track their products.

The flow of this data throughout the organization follows the process below, which is illustrated within the succeeding Software Architecture Diagram:

1. Data is sourced from customers using flat files transferred using Secure File Transfer Protocol (SFTP).
2. Data is then stored in AWS S3 instances and is encrypted at rest using AES-256.
3. Data validation checks are then performed on all data to ensure the data is complete and accurate.
4. Data is then normalized and put into a data schema.
5. Master data management (MDM) is performed and related data sources are linked.
6. Analytics are performed on the data to present it in the necessary format.
7. At this point, data is sent to Quickbase (Presentation Layer), and all customers log into Quickbase and utilize applications to view data.

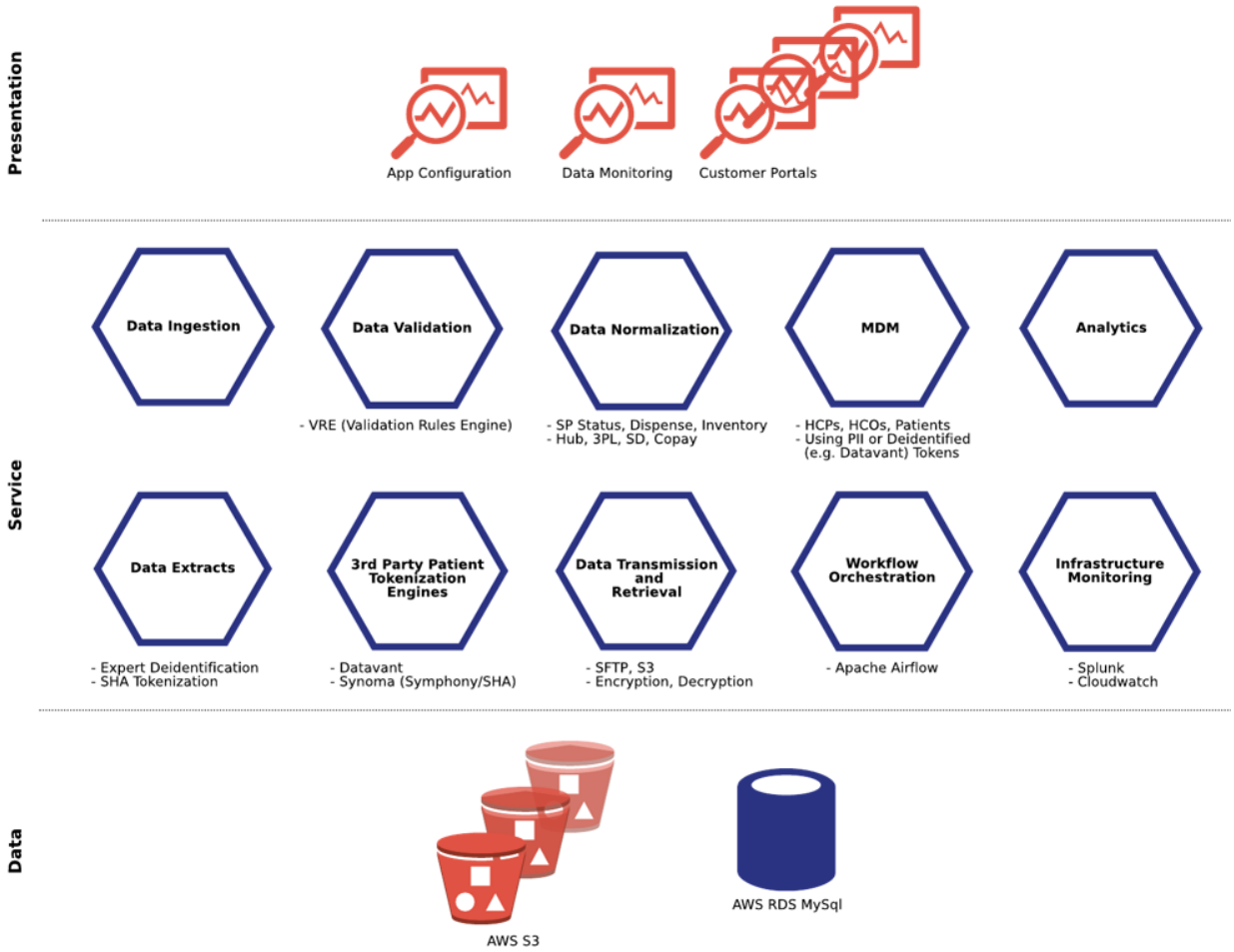

Figure 3: Claritas Rx's Software Architecture Diagram

Data Confidentiality and Classification

Claritas Rx identifies confidential information and personnel responsibilities regarding HIPAA regulations. Procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is required to be retained. The Data Classification Policy is used to assign all data handled by

Claritas Rx a classification that determines the data's handling, processing, encryption, and retention requirements. These data classifications include the following:

- Confidential—Reportable
- Confidential
- Internal Use Only
- Public

Data Encryption

Claritas Rx's encryption requirements and procedures (documented within the Encryption and Decryption Policy) are based on industry-accepted encryption best practices that comply with Federal Information Processing Standards (FIPS) 140-2 and include the following publications:

- National Institute of Standards and Technology (NIST) Special Publications (SP) 800-52 Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations
- NIST SP 800-77, Guide to IPsec Virtual Private Networks (VPNs)
- NIST SP 800-113, Guide to SSL VPNs

All data, PHI, and other sensitive information handled by the company is encrypted in transit via HTTPS and TLS v1.2 or greater where possible, per the Integrity Controls Policy. Connections and/or data transfers between Claritas Rx and its customers and third parties are secured using a Secure Shell (SSH) channel equipped with public/private key authentication and SFTP. All data, PHI, and other sensitive information handled by the company is encrypted at rest using 256-bit AES encryption keys, which are managed via AWS's Key Management System (KMS).

Data Retention

Claritas Rx retains all documentation required by the HIPAA regulations for a minimum of six years from the creation date or the date when the document was last in effect, whichever is later. Documentation and data retained using these standards include the following:

- Information security and privacy policies and procedures implemented to comply with HIPAA
- All documented settings, activities, and assessments required by HIPAA
- All data use agreements and other forms supporting HIPAA compliance
- All signed authorizations and, where applicable, written acknowledgements of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgements
- The Notice of Privacy Practices for entities that must provide them
- Documentation of the titles of the persons or offices responsible for HIPAA compliance, including not only those with overall responsibility for compliance, but also those responsible for receiving and processing requests for amendments by individuals, and those responsible for receiving and processing requests for an accounting by individuals
- Accounting of disclosures of PHI

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

The security and confidentiality categories and applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Security and confidentiality criteria and controls designed, implemented, and operated to meet them ensure that the system is protected against unauthorized access (both physical and logical). The controls supporting the applicable trust services security and confidentiality criteria are included in section IV of this report. Although the applicable trust services criteria and related controls are included in section IV, they are an integral part of Claritas Rx's description of its data aggregation and patient journey analytics software system.

Control Environment

Management Philosophy

Management communicates organizational vision, values, tone, and direction using several methods, including the dissemination of formal policies and the conduction of regular training programs and meetings., including the following:

- Company Lunch and Learns are conducted to discuss organizational goals and values and any identified issues and how these issues should be addressed.
- Personnel Town Hall meetings are conducted according to a formal cadence to communicate organizational tone, direction, vision, and values.
- The CEO uses a Slack channel to directly communicate issues or information with the organization related to compliance, performance, or alignment.
- Integrity and ethics standards are communicated to all personnel via a formal Code of Conduct and training programs that personnel are required to review and acknowledge or complete upon hire and annually thereafter.

Individual employee performance is monitored and managed by Team Leads. Monthly Town Hall meetings are conducted to discuss celebrations of success, achievements, special days/holidays, specific performance topics, goals, and the company's financial performance.

Security and Confidentiality Management

The organization's security and confidentiality requirements are managed using a combination of documented policies and procedures, management oversight, and network systems and hardware. These management practices are implemented in all areas of the control environment to protect systems, data, and personnel and to ensure compliance with industry best practices and standards.

Security and Confidentiality Policies

The Documentation Standards dictate personnel responsibilities regarding company documentation, including access control, document ownership, retention policy, document storage location(s), and backup processes and requirements.

All formal company policies and procedures must be annually reviewed and approved by either the Privacy Officer or the Information Security Officer. A Policy Review Log is maintained to document and track the review, update, and approval of all organizational policies, including the following information:

- Date of last review
- Revision status
- Date of last approval and by whom (the Security Officer and/or the Privacy Officer)

Policies are distributed to all new hires on their initial date of employment and must be acknowledged by the employee prior to their accessing any sensitive information, and policies are re-distributed to each workforce member during the month of their hire-date anniversary.

Personnel Security

The Employee Handbook defines processes and standards regarding personnel conduct and ethics, information confidentiality, new hire background checks, and progressive discipline. Personnel must review and acknowledge the Employee Handbook upon hire and annually thereafter, and this handbook is available for personnel review at all times via a shared drive.

A New Hire Orientation Standard Operating Procedure (SOP) is maintained and used to securely onboard all new employees and contractors and ensure that all required onboarding steps are completed. All new hires must agree to the Offer Letter and review and acknowledge the Employee Handbook and the Information Security Policy, and the completion of these tasks is documented and tracked via a Human Resources (HR) ticketing system.

Various background checks are completed on all new hires, including a Social Security (SSN) trace, a sex offender search, a global watchlist search, a national and county criminal searches, motor vehicle reports reviews, and work history and references validation. The performance of new hire background checks are guided by the Workforce Clearance Policy.

All personnel must complete security awareness and HIPAA security training programs upon hire and annually thereafter, and the completion of these training programs is guided by the Security Awareness and Training Policy. Incident Response Team members are required to complete incident response training annually that covers Claritas Rx's procedures for proper incident response, including roles and responsibilities and breach decision flow and documentation.

An Offboarding SOP and an Offboarding Checklist is maintained and used to securely offboard all employees and contractors and ensure that all required offboarding steps are completed.

Physical Security

Claritas Rx implements physical security controls within its two locations: South San Francisco, California and Lexington, Kentucky.

South San Francisco

Access to the South San Francisco location is restricted using key fobs and mechanical keys which are assigned to personnel using the principle of least privilege. Access to the South San

Francisco location requires access through two doors; access through the first door is restricted using key fobs, which are managed by the door manager; access through the second door can only be achieved using a mechanical key, of which only one exists and is in the possession of the CEO.

All access through the first door of the South San Francisco location is logged by the building manager, and these logs can be requested from the building manager for review. All access logs are retained for 30 days and document who accessed the location, the date and time of access, the ingress point used, and the action of the individual.

The South San Francisco location is equipped with security guards and security camera surveillance systems monitoring ingress and egress points at all times; a spreadsheet is used to log the review of any activity picked up by the cameras, and footage generated by these cameras are retained for 60 days for future review.

The South San Francisco location uses an Envoy Electronic Visitor Management System to document visitors to the location; logs generated by this system are retained for one year and document all relevant details regarding the visitor, including the following:

- The visitor's full name
- The location they visited
- Date and time in and out
- The purpose of the visit
- ID validation and a photo of the visitor
- Private notes
- Any applicable legal documents

Lexington

Access to the Lexington, KY location is controlled by a pushbutton key lock that is controlled by the building manager, and a key fob must be used to access the building after hours. The assignment of key fobs to personnel is documented and tracked for both locations, and all unused key fobs are securely stored within a locked file cabinet. The Lexington location utilizes a physical visitor log to document visitors, who are required to complete an entry in this log upon arrival.

Media Destruction

Claritas Rx's data and media erasure and destruction procedures are outlined within the Device and Media Controls Policy, which dictates persistent storage, media re-use, and media disposal requirements and processes. Prior to re-deploying or disposing of a workstation that has previously stored PHI, the hard drive of the device must be securely wiped by a workforce member or contracted IT vendor using use a wipe mechanism compliant with the industry-accepted media and data destruction best practice the NIST SP-88 Guidelines for Media Sanitation.

All workstations are sent to a third-party contractor to be destroyed or wiped of all data and media prior to reassignment, and device inventories are wiped using Department of Defense (DoD) standards. Secure shred bins are present in each location that personnel can use to

appropriately dispose of any confidential information; all documents in these bins are shredded by a third-party vendor regularly.

Change Management

The Change Management Policy is used to identify, request, approve, and implement all organizational infrastructure and configuration changes. This change management process is as follows:

1. Change requests must be submitted for approval and implementation by the Product Management and Engineering departments via a change request ticket.
2. Approved changes are entered into a backlog that is addressed and groomed by the Product Management and Engineering departments.
3. Estimated timelines and implementation tasks and assignments are established by the Engineering department.
4. All changes must be assessed and approved by the Quality Assurance (QA) department before the change can be implemented.

All changes are required to be requested, documented, and tracked to implementation via the use of an internal ticketing system, and these change request tickets document all relevant details regarding the change, including the following:

- Clearly identified roles and responsibilities
- Who authorized and approved the change
- What testing was performed prior to the implementation of the change
- A defined process for notifying customers prior to changes being made which may impact their service (if applicable)
- Post-installation validation processes and their results
- The back-out or recovery plans that were developed for the change

Configuration Management

The Configuration Standards, used to configure all organizational systems and devices, are based on the industry-accepted system configuration and hardening best practice NIST SP 800-128 Guide for Security Focused Configuration Management and Center for Internet Security (CIS) Benchmarks.

The company uses Infrastructure-as-a-Code (IaaC) and manages the configuration of this infrastructure using Ansible pre-configured playbooks. Standard Amazon Machine Images (AMIs) are used to implement server configuration standards in compliance with CIS standards. The Engineering Team is notified by Amazon whenever there is a new AMI version, and this new image is then incorporated into the Ansible playbooks for deployment.

Application Development

The formal Software Development Lifecycle (SDLC) is maintained and used to implement Claritas Rx's application and software development processes and requirements, which are based on the industry-accepted best practice Agile Methodology. Formal job descriptions are maintained for all Engineer and Developers specifying their roles and responsibilities, and logical access privileges and push to production capabilities are assigned based upon these descriptions and the principle of least privilege.

A secure source code repository is used to restrict access to source code, and code version control is implemented using branches. The organization also ensures the segregation of duties by logically and physically separating its application development, production, and staging environments using virtual private clouds (VPCs), separate AWS buckets, and security groups.

Developers must complete peer reviews and security checks on all code, code is then tested for functionality before push to production. Push to production capabilities are only assigned to DevOps personnel to ensure the segregation of duties and the security of the company's code and applications.

Application Change Management

The Change Management Policy is used to identify, request, approve, and implement all application and software development-related changes. This change management process is as follows:

1. Change requests for all application and software development-related changes must be submitted for approval and implementation by the Product Management and Engineering departments via a change request ticket.
2. Approved software development-related changes are entered into a backlog that is addressed and groomed by the Product Management and Engineering departments.
3. Estimated timelines and implementation tasks and assignments are established for all application and software development-related changes by the Engineering department.
4. All application and software development-related changes must be assessed and approved by the QA department before the change can be promoted to the application staging and production environments.
5. During deployment, all code is deployed to a pre-production environment and tested before they are deployed to production; scripts are used to pull down the latest release branch to deploy to the production environment.

All application and software development-related changes are required to be requested, documented, and tracked to implementation via the use of an internal ticketing system, and these change request tickets document all relevant details regarding the change, including the following:

- The subject of the change
- A description of the change
- Who requested the change
- Who approved the change and when
- The requested change date
- The change's priority rating
- The Developer or Team assigned to implement the change
- The employee or Team assigned to test the change
- Additional assignees, if any
- The change's implementation plan
- The change's test plan
- The change's rollback and/or rollforward plan

System Monitoring

The Vulnerability Management Policy dictates the required monitoring of all organizational systems and devices and the identification and management of detected vulnerabilities. Claritas Rx performs workstation vulnerability scanning monthly and employs a third party to conduct external penetration tests annually.

An intrusion detection system (IDS) is used that generates alerts upon detection of an intrusion, and these alerts are emailed to Security Engineers for investigation and remediation. The IDS also generates logs documenting all detected intrusions and incidents, and all logs are retained for future review. Other network monitoring and logging tools are also used to monitor and log the network activity of the organization; these activity logs document all relevant details for all network activity, including the following:

- Source IP
- Destination IP
- Destination port
- Protocol type
- Timestamp

Antivirus and anti-malware programs are implemented on all individual end-user systems and organizational servers and are configured in a manner preventing the altering of the programs' settings. The antivirus and anti-malware programs in use performs scans and updates daily, alerts personnel to any detected viruses or issues, and logs any detected issues for forensic analysis.

A firewall is used to prevent and detect any unauthorized traffic or activity on organizational systems and networks, and all users that connect to the network resources remotely must use multi-factor authentication (MFA), per the Person or Entity Authentication Policy.

Application Monitoring and Vulnerability Management

Claritas Rx performs periodic application vulnerability scanning and employs a third party to perform annual web application tests to test for common vulnerabilities. Code must be reviewed by at least one other developer during the peer review process to ensure functionality, and QA personnel must approve functionality testing before code is sent to deployment. The application development, staging, and production environments are unique and are logically and physically separated from each other using AWS accounts and VPCs.

Problem Management

The Incident Response Plan outlines the required procedure for handling detected incidents, including activation of the plan and detailed response actions for each organizational department. The plan describes the roles and responsibilities of the Incident Response Team members and their business units, which include representatives from management and the following departments:

- Engineering
- IT/Operations
- Customer Support
- HR

- Public Relations
- Finance

The Incident Response Team conducts an annual review of the Incident Response Plan, including reviewing team roles and responsibilities, the organization's definition of what constitutes a breach, classification of data, notification requirements, and reporting requirements. Formal incident notification and reporting requirements are defined and used by the Incident Response Team to ensure compliance with HIPAA and HITECH.

All critical or high vulnerabilities found during penetration tests are entered into a bug tracking system, are analyzed and assigned a severity rating, and are remediated according to this rating. Vulnerabilities assigned a severity of Critical must be mitigated and/or remediated as soon as possible and within a maximum of 30 days after detection. All detected incident and security breaches are documented and tracked until remediation using the Breach Investigation Log, which documents a description of the incident or breach, evidence of, any disseminated notifications regarding, and the actions taken to mitigate or remediate the issue.

An annual evaluation of all incidents that have been reported, including parties involved, the classification of involved data, the need of notification, and lessons learned following the resolution of the incident is performed; this review is guided by the Breach Evaluation Procedure.

Critical security patches are applied as soon as reasonably possible after release from the vendor, typically no later than the next weekly deployment, as required by the Patching Process. Patches on production systems may require complex testing and installation procedures, and in certain cases, risk mitigation rather than patching may be preferable. A risk assessment is conducted by the Security Officer, and any deviation from required patch implementation timelines is documented and authorized by the Security Officer.

Data Backup and Recovery

It is Claritas Rx's policy to respond to significant business disruptions by safeguarding employees' lives, protecting company property, performing operational assessments, and recovering and resuming operations as quickly as possible in order to continue providing products and services to its customers; the formal Business Continuity Plan and the Disaster Recovery Plan are used to guide these recovery processes, requirements, goals, and priorities. A Business Impact Analysis (BIA) is performed annually and as needed to identify recovery priorities such as recovery time objectives (RTOs) and recovery point objectives (RPOs); the Business Continuity Plan and the Disaster Recovery Plan are updated to reflect the results of the BIA.

All identified outages are assessed and assigned a severity rating used to determine required resolution timelines, including the following:

1. Severity 1: production servers or other mission critical systems are down and no workaround is immediately available
2. Severity 2: major functionality is impaired
3. Severity 3: partial or non-critical loss of business operations functionality
4. Severity 4: cosmetic issues with business operations functionality

Identified Recovery Response Teams are responsible for activating the plans when necessary, and the plans outline conditions for their activation and roles and responsibilities for these team members. The Business Continuity and the Disaster Recovery Plan also include a list of business-critical components and software and defined IT restoration procedures used to ensure the restoration of these components, software, and operational functions.

The Security Officer and the Disaster Recovery Team Lead establish criteria and determine a testing schedule for the performance of validation testing of the Business Continuity and the Disaster Recovery Plan. The plans are tested bi-annually and as needed using tabletop exercises and technical testing, and a disaster scenario is established and documented to use during this testing.

The validation and functional testing exercises of the Business Continuity and the Disaster Recovery Plan are also used as opportunities to train Recovery Response team personnel on their continuity and recovery roles and responsibilities, ensuring they can activate and carry out the plans as needed in the event of a business disruption or disaster.

Outcomes and lessons learned from the testing of the Business Continuity and the Disaster Recovery Plan are documented, tracked, and followed up on, and the plans are reviewed, updated, and approved of as necessary based on these findings and results.

Claritas Rx's business-critical systems, servers, and environments are backed up daily according to a formal backup process and schedule defined within the Backup Procedure. This backup schedule is as follows and includes the following systems, servers, and databases:

1. The following are stored and encrypted in Amazon S3, are moved to AWS Glacier storage after 10 days, and are retained indefinitely:
    a. Application servers
    b. Transfer servers
    c. SFTP servers
2. The following are backed up daily using volume snapshots at the drive level, and these encrypted backups are stored in AWS S3 using the volume snapshot functionality; 30 daily snapshots are maintained, and the oldest snapshot is deleted daily:
    a. Tableau servers
    b. VPN servers
3. RDS databases and MySQL instances are backed up independently daily using the RDS Snapshot service, and this snapshot backup is replaced daily with the new one.
4. The development environment is also backed up independently daily using the RDS Snapshot service, and this snapshot backup is replaced daily with the new one.
5. The production environment is backed up daily in snapshot form using AWS Backup Service, which encrypt and store the backups for five days.

System Account Management

Claritas Rx manages and authenticates logical access to all of its systems, workstations, environments, resources, and data using various logical access systems such as Open VPN, AWS IAM, and Google Admin. All users who access PHI via a computer at Claritas Rx is required to

use unique user identification, including a unique user account, ID, and password, per the Unique User Identification Policy. Formal password parameters are implemented on all company systems and workstations, including password length, complexity, expiration, and history requirements.

Logical access privileges are granted only on the basis of a valid business need, effectively implementing the principle of least privilege. Each employee's job description must be reviewed to determine the role and responsibilities of each individual with respect to PHI prior to the assignment and implementation of logical access privileges. All employee and contractor access is documented and tracked at a resource level (including per environment) to ensure all logical access to the company's systems, environments, and data is appropriate, and the Privacy Officer or their delegate reviews the access rights of all workforce members quarterly to confirm that they are aligned with the individual's current job role or function, and access rights are adjusted when necessary.

Personnel logical access privileges must be requested by the employee's manager, approved, and implemented after approval has been granted. All access requests are documented and tracked through approval and implementation, including documenting the level of access assigned to the employee and who approved of their logical access privileges.

The Terminations Policy and the Offboarding Standard Operating Procedures are used to revoke terminated or separating employee logical access privileges, and an Offboarding Checklist is used to ensure that all steps required within these procedures are completed per policy. A terminated or separated employee's logical access privileges are immediately revoked upon notification. The privilege revocation process includes the following required steps and procedures:

- Password access is immediately revoked.
- Access to all networks, systems and applications is revoked.
- The workforce member is removed from any systems or applications that process sensitive information.
- Access to any external systems where information about systems that store or process sensitive information may be stored.
- All digital certificates are revoked.
- Any tokens or smart cards issued to the workforce member are returned.
- Any keys and IDs provided to the workforce member during their employment are returned.
- If the workforce member is not leaving voluntarily and is provided access to their desk or office prior to leaving employment, such access may be supervised.

Customer Access

The Best Practices For New Claritas Customers document and is provided to customers to communicate the best use practices of Claritas Rx's application and services provided, including how customers manage their own access and accounts to these services, including access establishment and removal. A formal access establishment procedure is used by Claritas Rx when setting up customer's user accounts within its application; customers manage their own accounts and access after this initial setup. A Quickbase Customer User Removal

Procedure is used when revoking a customer's access to Claritas Rx's applications and services provided.

Risk Assessment Process

The risk assessment process, guided by the formal Risk Management Plan, is based on the industry-accepted risk management best practice NIST SP 800-30 and is performed at least annually and after any significant changes to the environment. The risk assessment focuses on threats and vulnerabilities that could impact the confidentiality, integrity, and availability of information and information systems, and addresses the likelihood of criminal fraud as a potential threat to the organization. Management reviews the results of each risk assessment and determines the transfer, avoidance, or acceptance of organizational risks and determines and approves of the company's risk tolerance level.

The Risk Management Team annually reviews the controls from the risk register that transfer, avoid, and mitigate risk to calibrate their effectiveness and implement adjustments as needed to meet the current needs and threats to the security posture of the organization. Management also annually reviews the effectiveness of controls that were put in place as a result of the previous risk assessment and determines new controls for threats that have been identified based on impact and likelihood.

Information and Communication Systems

The Information Security Policy addresses all organizational information security and technology requirements and procedures. Personnel are required to review and acknowledge the Information Security Policy upon hire and annually thereafter; the policy is available for review at all times via a Learning Management System. The Information Security Policy is distributed to business partners and associates as necessary as part of the partner's Security Risk Assessment process.

Internal that users can report potential complaints or security incidents by phone, email, in person, or confidentially by sending an anonymous report to the Security Officer or the Privacy Officer by US mail, per the Complaints and Breach Reports Policy.

Third-Party Breach Reporting

Business partners or associates are informed of and agree to their responsibilities for notifying Claritas Rx of a known or suspected security breach in their Business Associate Agreement, and the Privacy Policy posted on the company's public website includes contact information third parties can use to report potential complaints or security breaches.

Breach Reports are documented for each reported and identified security breach that includes a description of the incident and the remediation steps performed to remediate the incident. The report, identification, analysis, and remediation of all breaches are documented and tracked until completion with a Breach Investigation Log.

Customer Reports and Best Practices Documentation

A significant extract-transform-load (ETL) component must run smoothly regardless of any occasional data quality problems in the source files, and the organization has focused significant effort on making sure all batch jobs run as expected and are completed properly. Customer

reports are created so customers can monitor the performance of data analysis and batch jobs, and any issues with customer reports must be escalated to the Vice President (VP) of Engineering and the CEO.

Complementary User Entity controls are provided to customers that communicate the controls required from external users to securely utilize the services of Claritas Rx.

Vendor Management

The Vendor Management Procedure outlines required due diligence and ongoing compliance management procedures and standards. Prior to engagement with a third party, the organization completes an in-depth review of the potential vendor's security procedures. Potential vendors are required to complete a security questionnaire that is reviewed by the Information Security Team, who completes a Security Risk Assessment to determine if the potential vendor is compliant with the internal policies and standards of Claritas Rx.

In addition, the potential vendor may be required to provide evidence of any certifications, independent audit reports, or other evidence of a strong security profile, and any potential vendor that would potentially handle PHI or personally identifiable information (PII) on the organizations' behalf must provide a current security certification or audit report (ISO 27001, SOC 2 Type II, HITRUST, or equivalent). Each potential vendor is evaluated based on content provided, customization of the service, ease of use, documented issues, support metrics, and pricing; all information gathered during the due diligence process is captured within service-specific comparison spreadsheets.

Claritas Rx executes mutual non-disclosure agreements (MNDAs) with its third parties that define the scope of confidential information, requirements and obligations of both parties, the term of the agreement, and the handling of confidential information upon agreement termination. All executed MNDAs are managed and tracked via an internal contract management system.

Vendor service performance is evaluated, including their adherence to defined SLAs, any identified problems in functionality, their impact to Claritas Rx's business functions, and their compliance with applicable regulations and auditing frameworks. An annual review of all third-party service providers and vendors is conducted by requiring the relevant Subject Matter Expert or System Owner to answer several security questions, and the vendor's service delivery and compliance status is determined based on their answers. The questions are as follows:

1. Was their downtime beyond expected or outside the range stated in the SLA?
2. Have there been problems with functionality?
3. Does the vendor/product still meet our needs?

If/when a vendor or third-party service provider has failed to meet Claritas Rx's expectations, replacement of the vendor is considered and discussed by management.

Monitoring Controls

Company Key Performance Indicators (KPIs) are created based on metrics established from five-year company goals and are shared with the organization during regular meetings. Meetings are held to review company metrics and KPIs, and strategic priorities are established and assigned to

personnel during these meetings. Organizational goals are developed and used to develop the goals for each team and maintain alignment with the organization, and these include Team KPIs and Team Goal Areas; this information is shared via regular staff meetings.

IT personnel perform required daily operational security tasks to ensure the functioning of the company's business operations, including daily duties for application performance monitoring, security issue monitoring, job scheduling management, and data backup management. Application performance monitoring and job scheduling is performed by the Development Team, and daily log analysis is performed and automated. All daily operational security procedures are tracked within an internal ticketing system to ensure they are performed according to schedule.

Annual SOC 2 audits and HIPAA evaluations are conducted by independent auditing firms to assess Claritas Rx's internal controls and compliance. Executive management reviews the results of all audits and evaluations performed, and remediation efforts from previous audits are tracked manually by a Security Consultant via a spreadsheet. The Assigned Privacy Responsibility Policy outlines roles and responsibilities for personnel responsible for designing and developing system controls, and the Privacy Officer and Security Officer are responsible for the security controls, policies, and procedures of the organization.

Changes to the System During the Period

There were no changes that are likely to affect report users' understanding of the data aggregation and patient journey analytics software system during the period from January 1, 2021, through December 31, 2021.

COMPLEMENTARY USER-ENTITY CONTROLS

Claritas Rx's services are designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report. Claritas Rx's management makes control recommendations to user organizations and provides the means to implement these controls in many instances. Claritas Rx also provides best practice guidance to customers regarding control elements outside the sphere of Claritas Rx responsibility.

This section describes additional controls that should be in operation at user organizations to complement the Claritas Rx controls. Customer recommendations include:

- User organizations should implement sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with Claritas Rx.

- User organizations should ensure removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with Claritas Rx's services.

- Transactions for user organizations relating to Claritas Rx's services should be appropriately authorized, and transactions should be secure, timely, and complete.

- For user organizations sending data to Claritas Rx, data should be protected by appropriate methods to ensure confidentiality, privacy, integrity, availability, and non-repudiation. Claritas provides SFTP to support secure data transmissions and requires all non-SFTP transmissions to use TLS 1.2 or greater.

- User organizations should implement controls requiring additional approval procedures for critical transactions relating to Claritas Rx's services.

- User organizations should report to Claritas Rx in a timely manner any material changes to their overall control environment that may adversely affect services being performed by Claritas Rx.

- User organizations are responsible for notifying Claritas Rx in a timely manner of any changes to personnel directly involved with services performed by Claritas Rx. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by Claritas Rx.

- User organizations are responsible for adhering to the terms and conditions stated within their contracts with Claritas Rx.

- User organizations are responsible for developing, and if necessary, implementing a business continuity and disaster recovery plan that will aid in the continuation of services provided by Claritas Rx.

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Therefore, each customer's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

SECTION IV:
TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

APPLICABLE TRUST SERVICES CRITERIA RELEVANT TO SECURITY AND CONFIDENTIALITY

Although the applicable trust services criteria and related controls are presented in section IV, "Trust Services Categories, Criteria, Related Controls, and Tests of Controls," they are an integral part of Claritas Rx's system description throughout the period January 1, 2021, to December 31, 2021.

Security

The trust services criteria relevant to security address the need for information and systems to be protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the service organization's ability to achieve its service commitments and system requirements.

Security refers to the protection of

i. information during its collection or creation, use processing, transmission, and storage and

ii. systems that use electronic information to process, transmit or transfer, and store information to enable the achievement of Claritas Rx's service commitments and system requirements. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Confidentiality

The trust services criteria relevant to confidentiality address the need for information designated as confidential to be protected to achieve the service organization's service commitments and system requirements.

Confidentiality addresses Claritas Rx's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from Claritas Rx's control in accordance with management's objectives. Information is confidential if the custodian of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties. Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Trust Services Criteria for the Security and Confidentiality Categories			
Control Environment			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC1.1	The entity demonstrates a commitment to integrity and ethical values.		
CC1.1.1	Integrity and ethics standards are communicated to all personnel via a formal Code of Conduct and training programs that personnel are required to review and acknowledge or complete upon hire and annually theater.	Reviewed the 2021 Employee Handbook and verified that the Employee Handbook includes a Code of Conduct and must be acknowledged by all personnel upon hire and annually thereafter Interviewed the CEO regarding how the organization communicates ethics and verified that company values are discussed extensively during onboarding and that training provided through Litmos also covers the Code of Conduct and company values; this training is conducted during onboarding and annually thereafter Observed Employee Handbook acknowledgements completed by a sample of new hires (4 of 35) and verified that all new hires must acknowledge the Employee Handbook during the onboarding process Observed Employee Handbook acknowledgements completed by a sample of current personnel (9 of 85) and verified that all current personnel must acknowledge the Employee Handbook annually Observed the slide deck presented during new hire onboarding and verified that company values and code of conduct are covered during onboarding training	No Relevant Exceptions Noted
CC1.1.2	Management communicates organizational vision, values, tone, and direction using several methods, including the dissemination of formal policies and the conduction of regular training programs and meetings.	Reviewed the Employee Handbook and verified that the handbook includes the company's vision, values, and history, and must be acknowledged by all personnel upon hire and annually thereafter	No Relevant Exceptions Noted

		Interviewed the CEO regarding how management sets the tone and directions for the organization and verified that executive management sets the tone and direction for the company via onboarding presentations and formal policies; Lunch and Learns are conducted to discuss issues and how these issues should be addresses, values are worked into regular communications with all employees whether it is through daily, weekly, or monthly meetings or communications, and Town Hall meetings are conducted to further establish the mission and values across the organization Observed Town Hall Meeting Deck and verified that values and vision are communicated during the townhall meetings as well celebrating the success and accomplishments of those that best represent those values Observed Lunch and Learns and verified that regular training is conducted for the organization with further sets the tone and direction for the upcoming year Observed the slide deck presented during new hire onboarding and verified that company values and code of conduct are covered during onboarding training	
CC1.1.3	Company Lunch and Learns are conducted to discuss organizational goals and values and any identified issues and how these issues should be addressed.	Interviewed the CEO regarding how management sets the tone and direction for the organization and verified that executive management sets the tone and direction for the company via onboarding presentations and formal policies; Lunch and Learns are conducted to discuss issues and how these issues should be addresses, values are worked into regular communications with all employees whether it is through daily, weekly, or monthly meetings or communications, and Town Hall meetings are conducted	No Relevant Exceptions Noted

		to further establish the mission and values across the organization Observed Town Hall Meeting Deck and verified that values and vision are communicated during the townhall meetings as well celebrating the success and accomplishments of those that best represent those values Observed Lunch and Learns and verified that regular training is conducted for the organization with further sets the tone and direction for the upcoming year Observed the slide deck presented during new hire onboarding and verified that company values and code of conduct are covered during onboarding training	
CC1.1.4	Personnel Town Hall meetings are conducted according to a formal cadence to communicate organizational tone, direction, vision, and values.	Interviewed the CEO regarding how management sets the tone and direction for the organization and verified that executive management sets the tone and direction for the company via onboarding presentations and formal policies; Lunch and Learns are conducted to discuss issues and how these issues should be addresses, values are worked into regular communications with all employees whether it is through daily, weekly, or monthly meetings or communications, and Town Hall meetings are conducted to further establish the mission and values across the organization Observed Town Hall Meeting Deck and verified that values and vision are communicated during the townhall meetings as well celebrating the success and accomplishments of those that best represent those values Observed Lunch and Learns and verified that regular training is conducted for the organization with further sets the tone and direction for the upcoming year	No Relevant Exceptions Noted

		Observed the slide deck presented during new hire onboarding and verified that company values and code of conduct are covered during onboarding training	
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
CC1.2.1	Oversight of Claritas Rx's governance, strategic direction, and accountability is provided of its Board of Directors, which consists of five members.	Interviewed the Security & Compliance Consultant regarding the Board of Directors and verified that the Board is responsible for the governance, strategic direction, and accountability of the company and includes five members Observed Claritas Rx's public website and verified that the website lists the Board of Director's members	No Relevant Exceptions Noted
CC1.2.2	The Board meets quarterly to review the goals and objectives of the organization.	Interviewed the Security & Compliance Consultant regarding the Board of Directors and verified that the Board meets quarterly to review the goals and objectives of the organization Observed Claritas Rx's public website and verified that the website lists the Board of Director's members	No Relevant Exceptions Noted
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
CC1.3.1	Claritas Rx's traditional hierarchy, clear reporting lines, and functional departments are illustrated within a formal organizational chart.	Reviewed the organizational chart and verified that this chart illustrates the company's traditional hierarchy and its direct line of responsibility between security and executive leadership and that the ISO reports directly to the CEO, that the Security Team reports to the ISO, and that the Security Consultant reports to the CEO as well Interviewed the CEO regarding the organizational structure of the company and verified that the following functional areas are established: • Leadership—the Leadership Team, which reports to the CEO	No Relevant Exceptions Noted

		and is responsible for the other functional areas • Analytics—enables customers to gain insights from integrated self-service data sets • Corporate Strategy and Business Development—determines the company's goals and business strategy • Customer Success—represents the needs of the customer • Delivery & Operations—performs data operations and business analysis • Engineering—builds solutions based on needs defined by the Implementation and Product Teams • Finance—performs contract management and compliance • People Operations—performs HR functions • Product Management—determines product definitions and oversees product development Observed Zenefits and verified that the organizational chart is managed by Zenefits and reflects the organization's structure aligns with the interview results Observed a service delivery walkthrough and verified that the organization's structure aligns with the interview results	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
CC1.4.1	The Employee Handbook defines processes and standards regarding personnel conduct and ethics, information confidentiality, new hire background checks, and progressive discipline.	Reviewed the Employee Handbook and verified that the handbook defines processes and standards regarding personnel conduct and ethics, information confidentiality, new hire background checks, and progressive discipline Interviewed the Director of People Operations regarding the Employee	No Relevant Exceptions Noted

		Handbook and verified that the handbook must be acknowledged by all new employees during the onboarding process and annually thereafter and is available to all employees via Box shared drive Observed Employee Handbook acknowledgements completed by a sample of new hires (4 of 35) and verified that all new hires must acknowledge the Employee Handbook during the onboarding process Observed Employee Handbook acknowledgements completed by a sample of current personnel 9 of 85) and verified that all current personnel must acknowledge the Employee Handbook annually	
CC1.4.2	Personnel must review and acknowledge the Employee Handbook upon hire and annually thereafter, and this handbook is available for personnel review at all times via a shared drive.	Reviewed the Employee Handbook and verified that the handbook defines processes and standards regarding personnel conduct and ethics, information confidentiality, new hire background checks, and progressive discipline Interviewed the Director of People Operations regarding the Employee Handbook and verified that the handbook must be acknowledged by all new employees during the onboarding process and annually thereafter and is available to all employees via Box shared drive Observed Employee Handbook acknowledgements completed by a sample of new hires (4 of 35) and verified that all new hires must acknowledge the Employee Handbook during the onboarding process Observed Employee Handbook acknowledgements completed by a sample of current personnel 9 of 85) and verified that all current personnel must acknowledge the Employee Handbook annually	No Relevant Exceptions Noted

CC1.4.3	A New Hire Orientation SOP is maintained and used to securely onboard all new employees and contractors and ensure that all required onboarding steps are completed.	Reviewed the New Hire Orientation SOP (dated December 15, 2021) and the Employee Contracting SOP (June 14, 2021) and verified that these procedures list all steps that must be completed during the onboarding process for new employees and contractors Interviewed the Director of People Operations regarding the hiring and termination procedures for employees and contractors and verified that employees and contractors follow the same basic steps during the onboarding and offboarding process Observed Box and Zenefits accounts for a sample of new hires (4 of 35) and verified that onboarding documents and policies are assigned to each new hire for review and acknowledgement Observed Greenhouse accounts for a sample of new hires (4 of 35) and verified that references are obtained for all new hires	No Relevant Exceptions Noted
CC1.4.4	An Offboarding SOP and an Offboarding Checklist is maintained and used to securely offboard all employees and contractors and ensure that all required offboarding steps are completed.	Reviewed the Offboarding SOP (dated December 9, 2021) and verified that these procedures list all steps that must be completed during the offboarding process for new employees and contractors Interviewed the Director of People Operations regarding the hiring and termination procedures for employees and contractors and verified that employees and contractors follow the same basic steps during the onboarding and offboarding process Observed a sample of completed Offboarding Checklists (3 of 7) and verified that Checklists are utilized based on the Offboarding SOP to ensure that all steps are completed appropriately during the offboarding process	No Relevant Exceptions Noted

CC1.4.5	All new hires must agree to the Offer Letter and review and acknowledge the Employee Handbook and the Information Security Policy, and the completion of these tasks is documented and tracked via an HR ticketing system.	Interviewed the Director of People Operations regarding the forms, documents, and acknowledgements obtained during the new hire process and verified that during onboarding, new hires are required to review and acknowledge the Employee Handbook and the Information Security Policy, and these steps are tracked in Zenefits HR system and HR Application in Quickbase Observed Box and Zenefits accounts for a sample of new hires (4 of 35) and verified that all employees must agree to the Offer Letter, complete Information Security Training, and acknowledge the Employee Handbook as well as the Information Security Policy	No Relevant Exceptions Noted
CC1.4.6	Various background checks are completed on all new hires, including an SSN trace, a sex offender search, a global watchlist search, a national and county criminal searches, motor vehicle reports reviews, and work history and references validation.	Reviewed the Workforce Clearance Policy (dated June 29, 2021) and verified that all employees must have a background check performed per the Workforce Clearance Policy Interviewed the Director of People Operations regarding the background checks performed on all new hires and verified that all employees are subject to a background check; the organization uses a background check service from Checkr, which includes the following checks: • SSN trace • Sex offender search • Global watchlist search • National and county criminal searches • Motor vehicle reports reviews • Work history and references validation Observed background checks for a sample of new hires (4 of 35) and verified that all new hires had background checks completed during the audit period	No Relevant Exceptions Noted

CC1.4.7	The performance of new hire background checks are guided by the Workforce Clearance Policy.	Reviewed the Workforce Clearance Policy and verified that all employees must have a background check performed per the Workforce Clearance Policy Interviewed the Director of People Operations regarding the background checks performed on all new hires and verified that all employees are subject to a background check; the organization uses a background check service from Checkr, which includes the following checks: • SSN trace • Sex offender search • Global watchlist search • National and county criminal searches • Motor vehicle reports reviews • Work history and references validation Observed background checks for a sample of new hires (4 of 35) and verified that all new hires had background checks completed during the audit period	No Relevant Exceptions Noted
CC1.4.8	All personnel must complete security awareness and HIPAA security training programs upon hire and annually thereafter, and the completion of these training programs is guided by the Security Awareness and Training Policy.	Reviewed the Security Awareness and Training Policy (dated October 15, 2021) and verified that all personnel must complete security awareness and HIPAA security training programs upon hire and annually thereafter Interviewed the Director of People Operations regarding training programs of the organization and verified that all workforce members complete training assigned within the Litmos Learning Management System (LMS) and that all personnel must complete security awareness and HIPAA security training programs upon hire and annually thereafter Observed completed Litmos LMS training certificates for a sample of new hires (4 of 35) and current	No Relevant Exceptions Noted

		personnel (9 of 85) and verified that all personnel must complete security awareness and HIPAA security training programs upon hire and annually thereafter	
CC1.4.9	Incident Response Team members are required to complete incident response training annually that covers Claritas Rx's procedures for proper incident response, including roles and responsibilities and breach decision flow and documentation.	Reviewed the Incident Response Plan (dated May 27, 2021) and verified that Incident Response Team members are required to complete incident response training annually that covers Claritas Rx's procedures for proper incident response, including roles and responsibilities and breach decision flow and documentation Interviewed the Security & Compliance Consultant and verified that annual incident response training is mandatory for all Incident Response Team members Observed that the Breach Investigation Log is reviewed and used during incident response training programs to identify required incident resolution processes	No Relevant Exceptions Noted
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
CC1.5.1	The Documentation Standards dictate personnel responsibilities regarding company documentation, including access control, document ownership, retention policy, document storage location(s) and backup processes and requirements.	Reviewed the Documentation Standards (dated June 6, 2021) and verified that these standards dictate personnel responsibilities regarding company documentation, including access control, document ownership, retention policy, document storage location(s), and backup processes and requirements Interviewed the Security & Compliance Consultant regarding the methods for creating, approving, and maintaining the organization's policies and verified that all formal company policies and procedures must be annually reviewed and approved by either the Privacy Officer or the Information Security Officer	No Relevant Exceptions Noted

		Observed the Policy Review Log and verified that a spreadsheet log is kept of all of the organization's policies and the status of their review and approval process	
CC1.5.2	Policies are distributed to all new hires on their initial date of employment and must be acknowledged by the employee prior to their accessing any sensitive information, and policies are re-distributed to each workforce member during the month of their hire-date anniversary.	Reviewed the Information Security Policy (dated October 21, 2021) and verified that policies are distributed to all new hires on their initial date of employment and must be acknowledged by the employee prior to their accessing any sensitive information, and policies are re-distributed to each workforce member during the month of their hire-date anniversary Observed that organizational policies are communicated to personnel via document dissemination	No Relevant Exceptions Noted
CC1.5.3	All formal company policies and procedures must be annually reviewed and approved by either the Privacy Officer or the Information Security Officer.	Interviewed the Security & Compliance Consultant regarding the methods for creating, approving, and maintaining the organization's policies and verified that all formal company policies and procedures must be annually reviewed and approved by either the Privacy Officer or the Information Security Officer Observed the Policy Review Log and verified that a spreadsheet log is kept of all of the organization's policies and the status of their review and approval process	No Relevant Exceptions Noted
CC1.5.4	A Policy Review Log is maintained to document and track the review, update, and approval of all organizational policies.	Observed the Policy Review Log and verified that a spreadsheet log is kept of all of the organization's policies and the status of their review and approval process; this log documents the following details for each organizational policy: • The policy's date of last review • The policy's revision status • The policy's date of last approval and by whom (the Security Officer and/or the Privacy Officer)	No Relevant Exceptions Noted

CC1.5.5	Company KPIs are created based on metrics established from five-year company goals and are shared with the organization during regular meetings.	Interviewed the CEO regarding the monitoring activities performed by management to ensure operational quality and control and verified that company KPIs are created based on metrics established from five-year company goals, and are shared with the organization Observed a slide deck for a Town Hall meeting and verified that KPIs are reviewed with the organization including the goals, objectives, and financial performance metrics	No Relevant Exceptions Noted
CC1.5.6	Meetings are held to review company metrics and KPIs, and strategic priorities are established and assigned to personnel during these meetings.	Interviewed the CEO regarding the monitoring activities performed by management to ensure operational quality and control and verified that meetings are held to review company metrics and KPIs, and strategic priorities are established and assigned to personnel during these meetings Observed a slide deck for a Town Hall meeting and verified that KPIs are reviewed with the organization including the goals, objectives, and financial performance metrics	No Relevant Exceptions Noted
CC1.5.7	Organizational goals are developed and used to develop the goals for each team and maintain alignment with the organization, and these include Team KPIs and Team Goal Areas; this information is shared via regular staff meetings.	Interviewed the CEO regarding the monitoring activities performed by management to ensure operational quality and control and verified that organizational goals are developed and used to develop the goals for each team and maintain alignment with the organization, and these include Team KPIs and Team Goal Areas; this information is shared via regular staff meetings Observed a slide deck for a Town Hall meeting and verified that KPIs are reviewed with the organization including the goals, objectives, and financial performance metrics	No Relevant Exceptions Noted
CC1.5.8	Monthly Town Hall meetings are conducted to discuss celebrations of success, achievements, special days/holidays, specific	Interviewed the CEO regarding the monitoring activities performed by management to ensure operational quality and control and verified that	No Relevant Exceptions Noted

	performance topics, goals, and the company's financial performance.	monthly Town Hall meetings are conducted to discuss celebrations of success, achievements, special days/holidays, specific performance topics, goals, and the company's financial performance Observed a slide deck for a Town Hall meeting and verified that KPIs are reviewed with the organization including the goals, objectives, and financial performance metrics	
CC1.5.9	Individual employee performance is monitored and managed by Team Leads.	Interviewed the CEO regarding the monitoring activities performed by management to ensure operational quality and control and verified that individual employee performance is monitored and managed by Team Leads Observed the CEO Slack Channel and verified that the CEO has a direct channel to communicate any announcements and to update the organization consistently regarding compliance and performance	No Relevant Exceptions Noted
CC1.5.10	The CEO uses a Slack channel to directly communicate issues or information with the organization related to compliance, performance, or alignment.	Interviewed the CEO regarding the monitoring activities performed by management to ensure operational quality and control and verified that a CEO Slack channel is used to directly communicate with the organization related to compliance or issues within the organization regarding performance or alignment Observed the CEO Slack Channel and verified that the CEO has a direct channel to communicate any announcements and to update the organization consistently regarding compliance and performance Observed a slide deck for a Town Hall meeting and verified that KPIs are reviewed with the organization including the goals, objectives, and financial performance metrics	No Relevant Exceptions Noted

CC1.5.11	Customer reports are created so customers can monitor the performance of data analysis and batch jobs, and any issues with customer reports must be escalated to the VP of Engineering and the CEO.	Interviewed the Security & Compliance Consultant regarding the monitoring activities performed by the organization and verified that the organization produces customer reports that document data upload, analysis, and presentation metrics; any issues with customer reports must be escalated to the VP of Engineering and the CEO Observed the CEO Slack Channel and verified that the CEO has a direct channel to communicate any announcements and to update the organization consistently regarding compliance and performance Observed the Customer Report Dashboard and verified that customer reports are created so customers can monitor the performance of the data analysis and batch jobs	No Relevant Exceptions Noted
CC1.5.12	A significant ETL component must run smoothly regardless of any occasional data quality problems in the source files, and the organization has focused significant effort on making sure all batch jobs run as expected and are completed properly.	Interviewed the Security & Compliance Consultant regarding the monitoring activities performed by the organization and verified that the organization produces customer reports that document data upload, analysis, and presentation metrics; a significant ETL component must run smoothly regardless of any occasional data quality problems in the source files, and the organization has focused significant effort on making sure all batch jobs run as expected and are completed properly Observed the CEO Slack Channel and verified that the CEO has a direct channel to communicate any announcements and to update the organization consistently regarding compliance and performance Observed the Customer Report Dashboard and verified that customer reports are created so customers can monitor the performance of the data analysis and batch jobs	No Relevant Exceptions Noted

Trust Services Criteria for the Security and Confidentiality Categories			
Communication and Information			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
CC2.1.1	The Software Architecture Diagram illustrates the flow of data throughout the organization.	Reviewed the Software Architecture Diagram (dated February 3, 2021) and verified that this diagram illustrates the flow of data throughout the organization Interviewed the Principal Engineer regarding the data flow of the organization and verified that the flow is as follows: • Data is sourced from customers using flat files transferred using SFTP • Data is then stored in AWS S3 instances and is encrypted at rest using AES-256 • Data validation checks are then performed on all data to ensure the data is complete and accurate • Data is then normalized and put into a data schema • MDM is performed and related data sources are linked • Analytics are performed on the data to present it in the necessary format • At this point, data is sent to Quickbase (Presentation Layer),and all customers log into Quickbase and utilize applications to view data Observed a service delivery walkthrough and verified that the organization's structure aligns with the interview results	No Relevant Exceptions Noted
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
CC2.2.1	The Network Connectivity Diagram illustrates the company's networks, servers, and devices, and	Reviewed the Network Connectivity Diagram (dated August 14, 2021) and verified that the diagram is reviewed	No Relevant Exceptions Noted

	is reviewed and updated by the Principal Engineer annually and after any significant changes to the environment.	and updated by the Principal Engineer annually and after any significant changes to the environment Interviewed the Principal Engineer regarding the network diagram and verified that the production network is kept within a different Amazon account; the development and staging environments are kept in VPCs and buckets and are managed via security groups Observed the System Inventory and verified that it aligns with the network diagram and the design appropriately segregates traffic according to company policy and best practices	
CC2.2.4	All company systems, workstations, devices, and servers are documented and aggregated into a main System Inventory that documents, the use, function, and location of each item.	Interviewed the Security & Compliance Consultant regarding the management of system inventory and verified the following: • That workstations are managed by Robust Spreadsheets are supplied to the organization to verify against the internal Quickbase tracking of employee laptops, equipment, and key fobs • Servers are managed through the AWS Console in multiple Accounts • An internal tool is used to pull down all inventory into one list every eight hours to monitor the servers Observed the System Inventory and verified that it aligns with the network diagram and includes all virtual systems; the inventory provides a function or description of each and indicates the environment where each should be found	No Relevant Exceptions Noted
CC2.2.5	A formal software inventory is maintained that documents all of the company's critical software in use.	Interviewed the Principal Engineer regarding the management of software inventory and verified that the software inventory is managed through the use of coordinated software-as-a-service (SaaS) consoles	No Relevant Exceptions Noted

		Observed the software inventory and verified that the software observed aligns with the software inventory provided and the interview results regarding the management of the inventory	
CC2.2.6	The Assigned Privacy Responsibility Policy outlines roles and responsibilities for personnel responsible for designing and developing system controls.	Reviewed the Assigned Privacy Responsibility Policy and verified that the policy outlines roles and responsibilities for personnel responsible for designing and developing system controls Interviewed the Security & Compliance Consultant regarding the critical functions of the organization and verified that the Privacy Officer and Security Officer are responsible for the security controls, policies, and procedures of the organization Observed a service delivery walkthrough and verified that the organization's structure aligns with the interview results	No Relevant Exceptions Noted
CC2.2.7	The Privacy Officer and Security Officer are responsible for the security controls, policies, and procedures of the organization.	Reviewed the Assigned Privacy Responsibility Policy and verified that the policy outlines roles and responsibilities for personnel responsible for designing and developing system controls Interviewed the Security & Compliance Consultant regarding the critical functions of the organization and verified that the Privacy Officer and Security Officer are responsible for the security controls, policies, and procedures of the organization Observed a service delivery walkthrough and verified that the organization's structure aligns with the interview results	No Relevant Exceptions Noted
CC2.2.8	Internal users can report potential complaints or security incidents by phone, email, in person, or confidentially by sending an	Reviewed the Complaints and Breach Reports Policy and verified that users can report potential complaints or security incidents by phone, email, in	No Relevant Exceptions Noted

	anonymous report to the Security Officer or the Privacy Officer by US mail, per the Complaints and Breach Reports Policy.	person, or confidentially by sending an anonymous report to the Security Officer or the Privacy Officer by US mail Interviewed the Security & Compliance Consultant and verified that workforce members are provided with the Complaints and Breach Reports Policy as part of their new hire and annual training Observed the Breach Investigation Log and verified that the report, identification, analysis, and remediation of all breaches are documented and tracked until completion	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.		
CC2.3.1	Business partners or associates are informed of and agree to their responsibilities for notifying Claritas Rx of a known or suspected security breach in their Business Associate Agreement.	Interviewed the Security & Compliance Consultant and verified that business partners or associates are informed of and agree to their responsibilities for notifying Claritas Rx of a known or suspected security breach in their Business Associate Agreement Observed that the Privacy Policy posted on the company's public website includes contact information third parties can use to report potential complaints or security breaches	No Relevant Exceptions Noted
CC2.3.2	The Privacy Policy posted on the company's public website includes contact information third parties can use to report potential complaints or security breaches.	Interviewed the Security & Compliance Consultant and verified that business partners or associates are informed of and agree to their responsibilities for notifying Claritas Rx of a known or suspected security breach in their Business Associate Agreement Observed that the Privacy Policy posted on the company's public website includes contact information third parties can use to report potential complaints or security breaches	No Relevant Exceptions Noted

CC2.3.3	Breach Reports are documented for each reported and identified security breach that includes a description of the incident and the remediation steps performed to remediate the incident.	Observed a completed Breach Report and verified that the report includes a description of the incident and the remediation steps performed to remediate the incident	No Relevant Exceptions Noted
CC2.3.4	The report, identification, analysis, and remediation of all breaches are documented and tracked until completion with a Breach Investigation Log.	Observed the Breach Investigation Log and verified that the report, identification, analysis, and remediation of all breaches are documented and tracked until completion	No Relevant Exceptions Noted
CC2.3.5	Complementary User Entity controls are provided to customers that communicate the controls required from external users to securely utilize the services of Claritas Rx.	Reviewed the User Entity Controls and verified that the organization has developed Complementary User Entity controls that communicate the controls required from external users to securely use the services of Claritas Rx Observed that these User Entity Controls are provided to customers during onboarding	No Relevant Exceptions Noted
CC2.3.6	MSAs and/or SOWs are agreed upon with customers prior to engaging in any service offering.	Reviewed the following contracts and agreements and verified that Claritas Rx executes MSAs and/or SOWs with its customers: • MSA TerSera ClaritasRx (dated April 10, 2021) • SOW 1 TerSera ClaritasRx (dated January 1, 2021) • SOW 1 TerSera ClaritasRx Amended & Restated (dated October 15, 2021) • TPA Human Care Systems (HCS) ClaritasRx (dated October 29, 2021) Interviewed the CEO regarding the services and service commitments and verified that MSAs and SOWs are agreed upon with customers prior to engaging in any service offering; if SLAs are determined, they are agreed upon at a case-base-case basis and tracked by Customer Success Observed that SLA commitments are tracked within a spreadsheet and these	No Relevant Exceptions Noted

		commitments are made during contract negotiations; Claritas Rx classifies its SLA commitments into the following three categories: 1. System up-time commitments 2. Data processing commitments 3. Personnel availability commitments	
CC2.3.7	If SLAs are determined, they are agreed upon at a case-base-case basis and tracked by Customer Success.	Reviewed the following contracts and agreements and verified that Claritas Rx executes MSAs and/or SOWs with its customers: • MSA TerSera ClaritasRx (dated April 10, 2021) • SOW 1 TerSera ClaritasRx (dated January 1, 2021) • SOW 1 TerSera ClaritasRx Amended & Restated (dated October 15, 2021) • TPA HCS ClaritasRx (dated October 29, 2021) Interviewed the CEO regarding the services and service commitments and verified that MSAs and SOWs are agreed upon with customers prior to engaging in any service offering; if SLAs are determined, they are agreed upon at a case-base-case basis and tracked by Customer Success Observed that SLA commitments are tracked within a spreadsheet and these commitments are made during contract negotiations; Claritas Rx classifies its SLA commitments into the following three categories: 1. System up-time commitments 2. Data processing commitments 3. Personnel availability commitments	No Relevant Exceptions Noted
CC2.3.8	Claritas Rx classifies its customer SLA commitments into three categories: system up-time commitments, data processing commitments, and personnel availability commitments, and its commitments and SLAs with customers are documented and	Reviewed the SLA Audit Tracking spreadsheet and verified that customer SLAs are tracked via spreadsheet and managed accordingly Observed that SLA commitments are tracked within a spreadsheet and these commitments are made during contract	No Relevant Exceptions Noted

	tracked within customer-specific spreadsheets.	negotiations; Claritas Rx classifies its SLA commitments into the following three categories: 1. System up-time commitments 2. Data processing commitments 3. Personnel availability commitments	

Trust Services Criteria for the Security and Confidentiality Categories			
Risk Assessment			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
CC3.1.1	Claritas Rx is directly impacted by HIPAA as it processes, stores, or transmits ePHI, and a HIPAA evaluation is conducted annually to ensure organizational compliance with HIPAA requirements and standards.	Reviewed the HIPAA Compliance Attestation and verified that the organization acknowledges that it processes, stores, or transmits ePHI and conduct HIPAA evaluations annually to comply with HIPAA Security regulations that may impact the organization Interviewed the Security & Compliance Consultant regarding any regulatory measures that may impact the organization and verified that Claritas Rx is directly impacted by HIPAA, and an annual, review is conducted to ensure compliance with HIPAA requirements and standards Observed the results of an annual HIPAA evaluation and verified that management reviews the results of these evaluations to ensure Claritas Rx's compliance with HIPAA	No Relevant Exceptions Noted
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		
CC3.2.1	The risk assessment process, guided by the formal Risk Management Plan, is based on the industry-accepted risk management best practice NIST SP 800-30 and is performed at least annually and after any significant changes to the environment.	Reviewed the Risk Management Plan (dated March 24, 2021) and verified that the risk assessment process is based on the industry-accepted risk management best practice NIST SP 800-30 and is performed at least annually and after any significant changes to the environment Interviewed the Security & Compliance Consultant regarding the risk management program and verified that the organization annually reviews the effectiveness of controls put in place as a result of the previous risk assessment and determines new	No Relevant Exceptions Noted

		controls for identified threats based on impact and likelihood Observed the Risk Register and verified that the Risk Management Team annually reviews the controls from the risk register that transfer, avoid, and mitigate risk to calibrate their effectiveness and implement adjustments as needed to meet the current needs and threats to the security posture of the organization	
CC3.2.2	The risk assessment focuses on threats and vulnerabilities that could impact the confidentiality, integrity and availability of information and information systems.	Reviewed the Risk Management Plan and verified that the risk assessment process is based on NIST SP 800-30 and is performed at least annually and after significant changes to the environment Interviewed the Security & Compliance Consultant regarding the risk management program and verified that the risk assessment focuses on threats and vulnerabilities that could impact the confidentiality, integrity and availability of information and information systems Observed the Risk Register and verified that the Risk Management Team annually reviews the controls from the risk register that transfer, avoid, and mitigate risk to calibrate their effectiveness and implement adjustments as needed to meet the current needs and threats to the security posture of the organization	No Relevant Exceptions Noted
CC3.2.3	Management annually reviews the effectiveness of controls that were put in place as a result of the previous risk assessment and determines new controls for threats that have been identified based on impact and likelihood.	Interviewed the Security & Compliance Consultant regarding the risk management program and verified that the organization annually reviews the effectiveness of controls put in place as a result of the previous risk assessment and determines new controls for identified threats based on impact and likelihood Observed the Risk Register and verified that the Risk Management	No Relevant Exceptions Noted

		Team annually reviews the controls from the risk register that transfer, avoid, and mitigate risk to calibrate their effectiveness and implement adjustments as needed to meet the current needs and threats to the security posture of the organization	
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
CC3.3.1	The risk assessment addresses the likelihood of criminal fraud as a potential threat to the organization.	Reviewed the Risk Management Plan and verified that the risk assessment process is based on NIST SP 800-30 and is performed at least annually and after any significant changes to the environment Interviewed the Security & Compliance Consultant regarding the risk management program and verified that the risk assessment addresses the likelihood of criminal fraud as a potential threat to the organization Observed the Risk Register and verified that the Risk Management Team annually reviews the controls from the risk register that transfer, avoid, and mitigate risk to calibrate their effectiveness and implement adjustments as needed to meet the current needs and threats to the security posture of the organization	No Relevant Exceptions Noted
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.		
CC3.4.1	Management reviews the results of each risk assessment and determines the transfer, avoidance, or acceptance of organizational risks and determines and approves of the company's risk tolerance level.	Observed the Risk Register and verified that the Risk Management Team annually reviews the controls from the risk register that transfer, avoid, and mitigate risk to calibrate their effectiveness and implement adjustments as needed to meet the current needs and threats to the security posture of the organization	No Relevant Exceptions Noted
CC3.4.2	The Risk Management Team annually reviews the controls from the risk register that transfer, avoid, and mitigate risk to calibrate their effectiveness and implement	Observed the Risk Register and verified that the Risk Management Team annually reviews the controls from the risk register that transfer, avoid, and mitigate risk to calibrate	No Relevant Exceptions Noted

	adjustments as needed to meet the current needs and threats to the security posture of the organization	their effectiveness and implement adjustments as needed to meet the current needs and threats to the security posture of the organization	

Trust Services Criteria for the Security and Confidentiality Categories			
Monitoring Activities			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
CC4.1.1	Annual SOC 2 audits and HIPAA evaluations are conducted by independent auditing firms to assess Claritas Rx's internal controls and compliance.	Interviewed the Security & Compliance Consultant regarding any independent audits or regulatory exams that occurred within the last 12 months and verified that annual SOC 2 audits and HIPAA evaluations are conducted by independent auditing firms Observed logs from a webinar of SOC 2 findings and verified that executive management reviews the findings from previous SOC 2 audits Observed the Spreadsheet of Recommendations and verified that remediation efforts from previous audits are tracked manually by a Security Consultant	No Relevant Exceptions Noted
CC4.1.2	Executive management reviews the results of all audits and evaluations performed, and remediation efforts from previous audits are tracked manually by a Security Consultant via a spreadsheet.	Interviewed the Security & Compliance Consultant regarding any independent audits or regulatory exams that occurred within the last 12 months and verified that annual SOC 2 audits and HIPAA evaluations are conducted by independent auditing firms Observed logs from a webinar of SOC 2 findings and verified that executive management reviews the findings from previous SOC 2 audits Observed the Spreadsheet of Recommendations and verified that remediation efforts from previous audits are tracked manually by a Security Consultant	No Relevant Exceptions Noted
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.		

CC4.2.1	IT personnel perform required daily operational security tasks to ensure the functioning of the company's business operations, including daily duties for application performance monitoring, security issue monitoring, job scheduling management, and data backup management.	Reviewed the IT Operations Policy (dated August 13, 2021) and verified that the organization documents procedures for uses to store and process data supporting organization's products and services including daily duties for application performance monitoring, security issue monitoring, job scheduling management, and data backup management Interviewed the Security & Compliance Consultant and verified that application performance monitoring and job scheduling is performed by the Development Team and that daily log analysis is automated with Splunk Interviewed the Principal Engineer and verified that daily backups are automated and monitored in AWS and that any issues related to daily monitoring needing attention are entered and tracked in Jira Observed the use of Jira for managing issues	No Relevant Exceptions Noted
CC4.2.2	Application performance monitoring and job scheduling is performed by the Development Team, and daily log analysis is performed and automated.	Interviewed the Security & Compliance Consultant and verified that application performance monitoring and job scheduling is performed by the Development Team and that daily log analysis is automated with Splunk Interviewed the Principal Engineer and verified that daily backups are automated and monitored in AWS and that any issues related to daily monitoring needing attention are entered and tracked in Jira Observed the use of Jira for managing issues	No Relevant Exceptions Noted
CC4.2.3	All daily operational security procedures are tracked within an internal ticketing system to ensure	Interviewed the Security & Compliance Consultant and verified that application performance monitoring and job scheduling is	No Relevant Exceptions Noted

	they are performed according to schedule.	performed by the Development Team and that daily log analysis is automated with Splunk Interviewed the Principal Engineer and verified that daily backups are automated and monitored in AWS and that any issues related to daily monitoring needing attention are entered and tracked in Jira Observed the use of Jira for managing issues	

Trust Services Criteria for the Security and Confidentiality Categories			
Control Activities			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
CC5.1.1	Developers must complete peer reviews and security checks on all code, code is then tested for functionality before push to production.	Observed the company's software development process and its change management program and verified that Developers must complete peer reviews and security checks on all code, code is then tested for functionality before push to production	No Relevant Exceptions Noted
CC5.1.2	Formal job descriptions are maintained for all Engineer and Developers specifying their roles and responsibilities, and logical access privileges and push to production capabilities are assigned based upon these descriptions and the principle of least privilege.	Reviewed the Senior DevOps Engineer Job Description and verified that the Senior DevOps Engineer is responsible for the following: • Understand business processes, applications, and how data is gathered • Onboard new customer data using internal tools leveraging the Claritas Rx data pipeline • Build data expertise and own data quality • Develop an understanding of data models that provide intuitive analytics to customers • Use your expert coding skills in SQL and Python • Collaborate with multiple teams in high visibility roles and own the solution end-to-end • Support Claritas Rx's Production Data Aggregation environment in AWS including patching, monitoring, and alerting of systems • Architect and implement an Analytics Server environment running Jupyter Hub and Anaconda • Handle deployments and hotfixes to staging and production on a bi-monthly cadence • Support HIPAA and SOC 2 Type 2 audit activities	No Relevant Exceptions Noted

		• Support development system setup including application servers and databases • Automate system set up using Ansible • Manage SFTP and initial stack setup for Claritas Rx customers Interviewed the Security & Compliance Consultant regarding separation of duties in application development and verified that developers do not have access to the production environment and that only those developers that have been promoted to Dev/Ops Engineers have access to the production environment Observed Bitbucket and verified that implemented access control rights align with the policy and interview results and that only Engineers that are a part of the Dev/Ops Team have access to push to production capabilities	
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.		
CC5.2.1	The Information Security Policy addresses all organizational information security and technology requirements and procedures.	Reviewed the Information Security Policy (dated October 21, 2021) verified that the policy addresses all organizational information security and technology requirements and procedures Interviewed the Security & Compliance Consultant regarding the distribution and storage of the Information Security Policy and verified that all employees must acknowledge the Information Security Policy during onboarding and annually thereafter; the Information Security Policy is housed within their LMS and is also stored within the company shared Box system for access Observed Information Security Policy acknowledgements for a sample of new hires (4 of 35) and current	No Relevant Exceptions Noted

		personnel (9 of 85) and verified that all personnel are required to review and acknowledge the Information Security Policy upon hire and annually thereafter	
CC5.2.2	Personnel are required to review and acknowledge the Information Security Policy upon hire and annually thereafter, and the policy is available for review at all times via an LMS.	Reviewed the Information Security Policy and verified that policies are distributed to all new hires on their initial date of employment and must be acknowledged by the employee prior to their accessing any sensitive information; policies are re-distributed to each workforce member during the month of their hire-date anniversary Interviewed the Security & Compliance Consultant regarding the distribution and storage of the Information Security Policy and verified that all employees must acknowledge the Information Security Policy during onboarding and annually thereafter; the Information Security Policy is housed within their LMS and is also stored within the company shared Box system for access Observed Information Security Policy acknowledgements for a sample of new hires (4 of 35) and current personnel (9 of 85) and verified that all personnel are required to review and acknowledge the Information Security Policy upon hire and annually thereafter	No Relevant Exceptions Noted
CC5.2.3	The Information Security Policy is distributed to business partners and associates as necessary as part of the partner's Security Risk Assessment process.	Reviewed the Information Security Policy and verified that the Information Security Policy is distributed to business partners and associates as necessary during the partner's risk assessment Interviewed the Security & Compliance Consultant and verified that the Information Security Policy is distributed to business partners and associates as necessary as part of the partner's Security Risk Assessment process	No Relevant Exceptions Noted

		Observed Information Security Policy acknowledgements for a sample of new hires (4 of 35) and current personnel (9 of 85) and verified that all personnel are required to review and acknowledge the Information Security Policy upon hire and annually thereafter	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
CC5.3.1	It is Claritas Rx's policy to respond to significant business disruptions by safeguarding employees' lives, protecting company property, performing operational assessments, and recovering and resuming operations as quickly as possible in order to continue providing products and services to its customers; the formal Business Continuity Plan and the Disaster Recovery Plan are used to guide these recovery processes, requirements, goals, and priorities.	Reviewed the Business Continuity Plan (dated March 31, 2021) and the Disaster Recovery Plan and verified that it is Claritas Rx's policy to respond to significant business disruptions by safeguarding employees' lives, protecting company property, performing operational assessments, and recovering and resuming operations as quickly as possible in order to continue providing products and services to its customers; these plans are used to guide these processes, requirements, goals, and priorities Observed that Claritas Rx maintains a Business Continuity Plan and a Disaster Recovery Plan used to restore business operations in the event of a disaster or disruption	No Relevant Exceptions Noted
CC5.3.2	All identified outages are assessed and assigned a severity rating used to determine required resolution timelines.	Reviewed the Disaster Recovery Plan and verified that all identified outages are assessed and assigned a severity rating used to determine required resolution timelines; these severity ratings include the following: 1. Severity 1: production servers or other mission critical systems are down and no workaround is immediately available 2. Severity 2: major functionality is impaired 3. Severity 3: partial or non-critical loss of business operations functionality 4. Severity 4: cosmetic issues with business operations functionality	No Relevant Exceptions Noted

		Reviewed the Disaster Recovery Plan and verified that the following RTOs and RPOs are defined and maintained: • RPO of one hour • RTO of 48 hours from discovery of the outage Observed that Claritas Rx maintains a Business Continuity Plan and a Disaster Recovery Plan used to restore business operations in the event of a disaster or disruption	
CC5.3.3	A Business Impact Analysis (BIA) is performed as annually and as needed to identify recovery priorities such as RTO and RPOs, and the Business Continuity Plan and the Disaster Recovery Plan are updated to reflect the results of the BIA.	Reviewed the Disaster Recovery Plan and verified that the following RTOs and RPOs are defined and maintained: • RPO of one hour • RTO of 48 hours from discovery of the outage Reviewed the Business Continuity Plan and the Disaster Recovery Plan and verified that a BIA is performed annually and as needed to identify recovery priorities such as RTOs and RPOs, and the plans are updated to reflect the results of the BIA Observed that Claritas Rx maintains a Business Continuity Plan and a Disaster Recovery Plan used to restore business operations in the event of a disaster or disruption	No Relevant Exceptions Noted
CC5.3.4	The Business Continuity Plan and the Disaster Recovery Plan include a list of business-critical components and software and defined IT restoration procedures used to ensure the restoration of these components, software, and operational functions.	Reviewed the Business Continuity Plan and the Disaster Recovery Plan and verified that the plans include a list of business-critical components and software and defined IT restoration procedures used to ensure the restoration of these components, software, and operational functions Observed that Claritas Rx maintains a Business Continuity Plan and a Disaster Recovery Plan used to restore business operations in the event of a disaster or disruption	No Relevant Exceptions Noted

CC5.3.5	Identified Recovery Response Teams are responsible for activating the plans when necessary, and the plans outline conditions for their activation and roles and responsibilities for these team members.	Reviewed the Business Continuity Plan and the Disaster Recovery Plan and verified that identified Recovery Response Teams are responsible for activating the plans when necessary, and the plans outline conditions for their activation and roles and responsibilities for these team members Observed that Claritas Rx maintains a Business Continuity Plan and a Disaster Recovery Plan used to restore business operations in the event of a disaster or disruption	No Relevant Exceptions Noted
CC5.3.6	The Security Officer and the Disaster Recovery Team Lead establish criteria and determine a testing schedule for the performance of validation testing of the Business Continuity Plan and the Disaster Recovery Plan.	Reviewed the Disaster Recovery Plan and verified that the Security Officer and the Disaster Recovery Team Lead establish criteria and determine a testing schedule for the performance of validation testing of the Business Continuity Plan and the Disaster Recovery Plan Observed the Disaster Recovery Walkthrough PowerPoint and verified that when testing the Business Continuity Plan and the Disaster Recovery Plan, a disaster scenario is established and documented to use during testing	No Relevant Exceptions Noted
CC5.3.7	The plans are tested bi-annually and as needed using tabletop exercises and technical testing, and a disaster scenario is established and documented to use during this testing.	Reviewed the Disaster Recovery Plan and verified that the plans are tested bi-annually and as needed using tabletop exercises and technical testing Reviewed the 2021 Disaster Recovery Exercise Action Items document and verified that outcomes and lessons learned from the testing of the Business Continuity Plan and the Disaster Recovery Plan are documented, tracked, and followed up on, and the plans are reviewed and updated as necessary based on these findings and results Observed the Disaster Recovery Walkthrough PowerPoint and verified	No Relevant Exceptions Noted

		that when testing the Business Continuity Plan and the Disaster Recovery Plan, a disaster scenario is established and documented to use during testing	
CC5.3.8	The validation and functional testing exercises of the Business Continuity Plan and the Disaster Recovery Plan are also used as opportunities to train Recovery Response team personnel on their continuity and recovery roles and responsibilities, ensuring they can activate and carry out the plans as needed in the event of a business disruption or disaster.	Reviewed the Disaster Recovery Plan and verified that the validation and functional testing exercises of the Business Continuity Plan and the Disaster Recovery Plan are also used as opportunities to train Recovery Response team personnel on their continuity and recovery roles and responsibilities, ensuring they can activate and carry out the plans as needed in the event of a business disruption or disaster Reviewed the 2021 Disaster Recovery Exercise Action Items document and verified that outcomes and lessons learned from the testing of the Business Continuity Plan and the Disaster Recovery Plan are documented, tracked, and followed up on, and the plans are reviewed and updated as necessary based on these findings and results Observed the Disaster Recovery Walkthrough PowerPoint and verified that when testing the Business Continuity Plan and the Disaster Recovery Plan, a disaster scenario is established and documented to use during testing	No Relevant Exceptions Noted
CC5.3.9	Outcomes and lessons learned from the testing of the Business Continuity Plan and the Disaster Recovery Plan are documented, tracked, and followed up on, and the plans are reviewed, updated, and approved of as necessary based on these findings and results.	Reviewed the 2021 Disaster Recovery Exercise Action Items document and verified that outcomes and lessons learned from the testing of the Business Continuity Plan and the Disaster Recovery Plan are documented, tracked, and followed up on, and the plans are reviewed and updated as necessary based on these findings and results Observed the Disaster Recovery Walkthrough PowerPoint and verified	No Relevant Exceptions Noted

		that when testing the Business Continuity Plan and the Disaster Recovery Plan, a disaster scenario is established and documented to use during testing	
CC5.3.10	Claritas Rx's business-critical systems, servers, and environments are backed up daily according to a formal backup process and schedule defined within the Backup Procedure.	Reviewed the Backup Procedure (dated November 30, 2021) and verified that Claritas Rx performs the following backups of its infrastructure in all environments: • Application servers are backed up daily, are stored and encrypted in Amazon S3, are moved to AWS Glacier storage after 10 days, and are retained indefinitely • Transfer servers are backed up daily, are stored and encrypted in Amazon S3, are moved to AWS Glacier storage after 10 days, and are retained indefinitely • SFTP servers are backed up daily, are stored and encrypted in Amazon S3, are moved to AWS Glacier storage after 10 days, and are retained indefinitely • Tableau servers are backed up daily using volume snapshots at the drive level, and these encrypted backups are stored in AWS S3 using the volume snapshot functionality; 30 daily snapshots are maintained, and the oldest snapshot is deleted daily • VPN servers are backed up daily using volume snapshots at the drive level, and these encrypted backups are stored in AWS S3 using the volume snapshot functionality; 30 daily snapshots are maintained, and the oldest snapshot is deleted daily • RDS databases and MySQL instances are backed up independently daily using the RDS Snapshot service, and this snapshot backup is replaced daily with the new one • The development environment is also backed up independently	No Relevant Exceptions Noted

		daily using the RDS Snapshot service, and this snapshot backup is replaced daily with the new one • The production environment is backed up daily in snapshot form using AWS Backup Service, which encrypt and store the backups for five days Interviewed the Security & Compliance Consultant regarding the data backups of the organization and verified that all backups are conducted through AWS, are performed and collected daily, and are retained according to the policy schedule Observed the AWS Production Account and verified that AWS S3 Buckets have encryption enabled and that the following systems and environments are backed up on a daily basis: • Application servers • Transfer servers • SFTP servers • Tableau servers • VPN servers • RDS databases • MySQL instances • The development environment • The production environment Observed a sample of production servers (8 of 19) and verified that all production servers are backed up daily per company policy Observed Amazon RDS Data Restoration Testing and verified that database restoration testing was performed on December 20, 2021, and that these backups were restored to a development account for testing and were restored successful with no detected issues	

Trust Services Criteria for the Security and Confidentiality Categories			
Logical and Physical Access Controls			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
CC6.1.1	Claritas Rx manages and authenticates logical access to all of its systems, workstations, environments, resources, and data using various logical access systems such as Open VPN, AWS IAM, and Google Admin.	Interviewed the Security & Compliance Consultant regarding the logical access systems used by the organization and verified that all workstations maintain local accounts for access and that users are managed using OpenVPN for network access, AWS IAM for Amazon resources, and Google Admin for access to GSuite Observed OpenVPN and verified that OpenVPN is used in conjunction with MFA to authenticate access to network resources Observed Google Admin and verified that Google Admin is used to authenticate access to business applications and documentation Observed workstation configurations and verified that local accounts are used to access the workstations of the organization and that these workstations are regulated through policies within Barracuda Managed Workplace Observed AWS IAM and verified that all access to the AWS console ais managed with IAM	No Relevant Exceptions Noted
CC6.1.2	All users who access PHI via a computer at Claritas Rx is required to use unique user identification, including a unique user account, ID, and password, per the Unique User Identification Policy.	Reviewed the Unique User Identification Policy (dated June 29, 2021) and verified that each individual who access PHI via computer at Claritas Rx is required to use unique user identification, including a unique user account, ID, and password	No Relevant Exceptions Noted

		Observed User Lists and verified that all users were assigned unique user IDs	
CC6.1.3	All employee and contractor access is documented and tracked at a resource level (including per environment) to ensure all logical access to the company's systems, environments, and data is appropriate.	Interviewed the Security & Compliance Consultant regarding how the organization authorizes and implements user IDs and verified that all employee and contractor access is documented and tracked at a resource level (including per environment) to ensure all logical access to the company's systems, environments, and data is appropriate Observed Quickbase access requests for a sample of new hires (4 of 35) and verified that Quickbase is used to track all requests for user IDs and access to system resources; access is authorized by the associated manager and is based on the predefined roles within the organization	No Relevant Exceptions Noted
CC6.1.4	The formal Software Development Lifecycle (SDLC) is maintained and used to implement Claritas Rx's application and software development processes and requirements, which are based on the industry-accepted best practice Agile Methodology.	Reviewed the SDLC (dated June 29, 2021) and verified that the organization uses the Agile Methodology for application and software development	No Relevant Exceptions Noted
CC6.1.5	A secure source code repository is used to restrict access to source code, and code version control is implemented using branches.	Interviewed the Security & Compliance Consultant regarding the source code repository and version control and verified that Bitbucket is used as the source code repository and GitFlow manages the version control using branches Observed Bit Bucket and verified that access control is performed through branch permissions and that only DevOps personnel have access to push to production Observed GitFlow and verified that versioning is managed through the use of branches	No Relevant Exceptions Noted

CC6.1.6	Push to production capabilities are only assigned to DevOps personnel to ensure the segregation of duties and the security of the company's code and applications.	Interviewed the Security & Compliance Consultant regarding the source code repository and version control and verified that Bitbucket is used as the source code repository and GitFlow manages the version control using branches Observed Bit Bucket and verified that access control is performed through branch permissions and that only DevOps personnel have access to push to production Observed GitFlow and verified that versioning is managed through the use of branches	No Relevant Exceptions Noted
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
CC6.2.1	Personnel logical access privileges must be requested by the employee's manager, approved, and implemented after approval has been granted.	Reviewed the Unique User Identification Policy and verified that each individual who accesses PHI via computer at Claritas Rx is required to use unique user identification, including a unique user account, ID, and password Interviewed the Security & Compliance Consultant regarding how the organization authorizes and implements user IDs and verified that access requests are made by the employee's manager and tracked in Quickbase; once the request is approved, notifications are sent to the person implementing the access, and once the access has been granted to the user for the given resource, the record is updated to reflect when their access was granted and by whom Observed Quickbase access requests for a sample of new hires (4 of 35) and verified that Quickbase is used to track all requests for user IDs and access to system resources; access is authorized by the associated manager and is based	No Relevant Exceptions Noted

		on the predefined roles within the organization Observed User Lists and verified that all users were assigned unique user IDs	
CC6.2.2	All access requests are documented and tracked through approval and implementation, including documenting the level of access assigned to the employee and who approved of their logical access privileges.	Interviewed the Security & Compliance Consultant regarding how the organization authorizes and implements user IDs and verified that access requests are made by the employee's manager and tracked in Quickbase; once the request is approved, notifications are sent to the person implementing the access, and once the access has been granted to the user for the given resource, the record is updated to reflect when their access was granted and by whom Observed Quickbase access requests for a sample of new hires (4 of 35) and verified that Quickbase is used to track all requests for user IDs and access to system resources; access is authorized by the associated manager and is based on the predefined roles within the organization Observed User Lists and verified that all users were assigned unique user IDs	No Relevant Exceptions Noted
CC6.2.3	Formal password parameters are implemented on all company systems and workstations, including password length, complexity, expiration, and history requirements.	Observed the implemented AWS IAM password policy and verified that the following password parameters are implemented on all company systems and workstations: • Minimum password length is 14 characters • Password complexity requirements are outlined • Passwords expire in 90 days • Users may change their own passwords • Password history remembers last 24 passwords	No Relevant Exceptions Noted

CC6.2.4	A formal access establishment procedure is used by Claritas Rx when setting up a customer's user account within its application; customers manage their own accounts and access after this initial setup.	Reviewed the Quickbase Customer User Removal Procedure and verified that this procedure is used by Claritas Rx when setting up a customer's user account within its application; customers manage their own accounts and access after this initial setup Interviewed the VP of Delivery and Operations regarding how customers are registered and deregistered and verified that users are setup by the organization in the Quickbase application; Customer Success Team Members are assigned to every customer account and work with customers to create new users and delete old ones as needed Observed Quickbase and verified that all customer users are managed by the organization through Customer Success Team Members, and Quickbase is utilized for this logical access	No Relevant Exceptions Noted
CC6.2.5	The Best Practices For New Claritas Customers document and is provided to customers to communicate the best use practices of Claritas Rx's application and services provided, including how customers manage their own access and accounts to these services, including access establishment and removal.	Reviewed the Best Practices For New Claritas Customers document and verified that it is provided to customers to communicate the best use practices of Claritas Rx's application and services provided, including how customers manage their own access and accounts to these services, including access establishment and removal Interviewed the VP of Delivery and Operations regarding how customers are registered and deregistered and verified that users are setup by the organization in the Quickbase application; Customer Success Team Members are assigned to every customer account and work with customers to create new users and delete old ones as needed	No Relevant Exceptions Noted
CC6.2.6	A Quickbase Customer User Removal Procedure is used when revoking a customer's access to	Reviewed the Quickbase Customer User Removal Procedure and verified that this procedure is used by Claritas	No Relevant Exceptions Noted

	Claritas Rx's applications and services provided.	Rx when decommissioning customer's user accounts within its application Interviewed the VP of Delivery and Operations regarding how customers are registered and deregistered and verified that users are setup by the organization in the Quickbase application; Customer Success Team Members are assigned to every customer account and work with customers to create new users and delete old ones as needed	
CC6.2.7	A terminated or separated employee's logical access privileges are immediately revoked upon notification.	Reviewed the Terminations Policy (dated October 15, 2021) and verified that the Human Resources (HR) and IT departments coordinate their activities to ensure the following procedures are performed upon an employee's termination or separation: • Password access is immediately revoked • Access to all networks, systems and applications is revoked • The workforce member is removed from any systems or applications that process sensitive information • Access to any external systems where information about systems that store or process sensitive information may be stored • All digital certificates are revoked • Any tokens or smart cards issued to the workforce member are returned • Any keys and IDs provided to the workforce member during their employment are returned • If the workforce member is not leaving voluntarily and is provided access to their desk or office prior to leaving employment, such access may be supervised Interviewed the Security & Compliance Consultant regarding the immediate revocation of access for all	No Relevant Exceptions Noted

		terminated users and verified that Offboarding Standard Operating Procedures are followed in conjunction with Quickbase to make sure that all steps are completed appropriately during the offboarding process including the immediate termination of access to system resources Observed offboarding checklists and verified that immediate termination of access is required for all terminated employees of the organization Observed Quickbase and verified that access terminations are tracked within the Quickbase application Observed Quickbase access for a sample of terminated employees (3 of 7) and verified that all terminated employee access was revoked at the point of termination during the audit period	
CC6.2.8	The Terminations Policy and the Offboarding Standard Operating Procedures are used to revoke terminated or separating employee logical access privileges, and an Offboarding Checklist is used to ensure that all steps required within these procedures are completed per policy.	Reviewed the Terminations Policy and verified that the HR IT departments coordinate their activities to ensure the following procedures are performed upon an employee's termination or separation: • Password access is immediately revoked • Access to all networks, systems and applications is revoked • The workforce member is removed from any systems or applications that process sensitive information • Access to any external systems where information about systems that store or process sensitive information may be stored • All digital certificates are revoked • Any tokens or smart cards issued to the workforce member are returned • Any keys and IDs provided to the workforce member during their employment are returned	No Relevant Exceptions Noted

		• If the workforce member is not leaving voluntarily and is provided access to their desk or office prior to leaving employment, such access may be supervised Interviewed the Security & Compliance Consultant regarding the immediate revocation of access for all terminated users and verified that Offboarding Standard Operating Procedures are followed in conjunction with Quickbase to make sure that all steps are completed appropriately during the offboarding process including the immediate termination of access to system resources Observed offboarding checklists and verified that immediate termination of access is required for all terminated employees of the organization Observed Quickbase and verified that access terminations are tracked within the Quickbase application Observed Quickbase access for a sample of terminated employees (3 of 7) and verified that all terminated employee access was revoked at the point of termination during the audit period	
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
CC6.3.1	Each employee's job description must be reviewed to determine the role and responsibilities of each individual with respect to PHI prior to the assignment and implementation of logical access privileges.	Reviewed the Access Management Policy and verified that each employee's job description must be reviewed to determine the role and responsibilities of each individual with respect to PHI prior to the assignment and implementation of logical access privileges Interviewed the Security & Compliance Consultant regarding	No Relevant Exceptions Noted

		access rights and privileges granted to user IDs and verified that the organization uses the principle of least privilege Observed the results of four quarterly access reviews and verified that quarterly user access reviews are conducted that document the list of users, groups they belong to, their access to the development or production environments if applicable, and any notes on adjustments that must be made to access rights and privileges	
CC6.3.2	Logical access privileges are granted only on the basis of a valid business need, effectively implementing the principle of least privilege.	Reviewed the Access Management Policy and verified that logical access privileges are granted only on the basis of a valid business need, effectively implementing the principle of least privilege Interviewed the Security & Compliance Consultant regarding access rights and privileges granted to user IDs and verified that the organization uses the principle of least privilege Observed the results of four quarterly access reviews and verified that quarterly user access reviews are conducted that document the list of users, groups they belong to, their access to the development or production environments if applicable, and any notes on adjustments that must be made to access rights and privileges	No Relevant Exceptions Noted
CC6.3.3	The Privacy Officer or their delegate reviews the access rights of all workforce members quarterly to confirm that they are aligned with the individual's current job role or function, and access rights are adjusted when necessary.	Interviewed the Security & Compliance Consultant regarding access rights and privileges granted to user IDs and verified that the Privacy Officer or their delegate reviews the access rights of all workforce members quarterly to confirm that they are aligned with the individual's current job role or function Observed the results of four quarterly access reviews and verified that	No Relevant Exceptions Noted

		quarterly user access reviews are conducted that document the list of users, groups they belong to, their access to the development or production environments if applicable, and any notes on adjustments that must be made to access rights and privileges	
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
CC6.4.1	Access to the South San Francisco location is restricted using key fobs and mechanical keys which are assigned to personnel using the principle of least privilege.	Interviewed the Security & Compliance Consultant regarding the physical security controls of the organization and verified that access to the South San Francisco location requires access through two doors; access through the first door is restricted using key fobs, which are managed by the door manager; access through the second door can only be achieved using a mechanical key, of which only one exists and is in the possession of the CEO Observed that all access through the first door is logged by the building manager, and these logs can be requested from the building manager for review	No Relevant Exceptions Noted
CC6.4.2	All access through the first door of the South San Francisco location is logged by the building manager, and these logs can be requested from the building manager for review.	Interviewed the Security & Compliance Consultant regarding the physical security controls of the organization and verified that access to the South San Francisco location requires access through two doors; access through the first door is restricted using key fobs, which are managed by the door manager; access through the second door can only be achieved using a mechanical key, of which only one exists and is in the possession of the CEO Observed that all access through the first door is logged by the building manager, and these logs can be requested from the building manager for review	No Relevant Exceptions Noted

		Observed an access control log for the South San Francisco location and verified that these logs are retained for 30 days and document who accessed the location, the date and time of access, the ingress point used, and the action of the individual	
CC6.4.3	All access logs are retained for 30 days and document who accessed the location, the date and time of access, the ingress point used, and the action of the individual.	Observed that all access through the first door is logged by the building manager, and these logs can be requested from the building manager for review Observed an access control log for the South San Francisco location and verified that these logs are retained for 30 days and document who accessed the location, the date and time of access, the ingress point used, and the action of the individual	No Relevant Exceptions Noted
CC6.4.4	The South San Francisco location is equipped with security guards and security camera surveillance systems monitoring ingress and egress points at all times; a spreadsheet is used to log the review of any activity picked up by the cameras, and footage generated by these cameras are retained for 60 days for future review.	Reviewed an email from Property Manager and verified that security guards are supplied for the South San Francisco location at all times Observed that the South San Francisco location is equipped with security guards and security camera surveillance systems monitoring ingress and egress points at all times; a spreadsheet is used to log the review of any activity picked up by the cameras Observed Video Retention Review Logs from Reolink and verified that footage generated by the South San Francisco location's security camera surveillance systems are retained for 60 days	No Relevant Exceptions Noted
CC6.4.5	Access to the Lexington, KY location is controlled by a pushbutton key lock that is controlled by the building manager, and a key fobs must be used to access the building after hours.	Observed the Lexington, KY location and verified that access to this location is controlled by a pushbutton key lock that is controlled by the building manager, and a key fobs must be used to access the building after hours	No Relevant Exceptions Noted

CC6.4.6	The assignment of key fobs to personnel is documented and tracked for both locations, and all unused key fobs are securely stored within a locked file cabinet.	Observed that the assignment of key fobs to personnel is documented and tracked for both locations, and all unused key fobs are securely stored within a locked file cabinet	No Relevant Exceptions Noted
CC6.4.7	The South San Francisco location uses an Envoy Electronic Visitor Management System to document visitors to the location; logs generated by this system are retained for one year and document all relevant details regarding the visitor.	Interviewed the Security & Compliance Consultant regarding the physical security controls of the organization and verified that the South San Francisco location uses an Envoy Electronic Visitor Management System and the Lexington location utilizes a paper book to record any users that visit Observed documented visitor logs and verified that logs are obtained through an iPad Envoy System; these logs are retained for one year and document the following information for each visitor: • The visitor's full name • The location they visited • Date and time in and out • The purpose of the visit • ID validation and a photo of the visitor • Private notes • Any applicable legal documents	No Relevant Exceptions Noted
CC6.4.8	The Lexington location utilizes a physical visitor log to document visitors, who are required to complete an entry in this log upon arrival.	Interviewed the Security & Compliance Consultant regarding the physical security controls of the organization and verified that the South San Francisco location uses an Envoy Electronic Visitor Management System and the Lexington location utilizes a paper book to record any users that visit Observed documented visitor logs and verified that logs are obtained through an iPad Envoy System; these logs are retained for one year and document the following information for each visitor: • The visitor's full name • The location they visited • Date and time in and out • The purpose of the visit	No Relevant Exceptions Noted

		• ID validation and a photo of the visitor • Private notes • Any applicable legal documents	
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.		
CC6.5.1	Prior to re-deploying or disposing of a workstation that has previously stored PHI, the hard drive of the device must be securely wiped by a workforce member or contracted IT vendor using use a wipe mechanism compliant with the industry-accepted media and data destruction best practice the NIST SP-88 Guidelines for Media Sanitation.	Reviewed the Device and Media Controls Policy (dated October 15, 2021) and verified that prior to re-deploying or disposing of a workstation that has previously stored PHI, the hard drive of the device must be securely wiped by a workforce member or contracted IT vendor using use a wipe mechanism compliant with the industry-accepted media and data destruction best practice the NIST SP-88 Guidelines for Media Sanitation Observed Robust Inventory Management and verified that inventory is wiped using DoD standards when devices are reassigned Observed the presence of shred bins in each location that can be used to appropriately dispose of any confidential information	No Relevant Exceptions Noted
CC6.5.2	all workstations are sent to a third-party contractor to be destroyed or wiped of all data and media prior to reassignment, and device inventories are wiped using Department of Defense (DoD) standards.	Interviewed the Security & Compliance Consultant verified that all workstations are sent to a third-party contractor to be destroyed or wiped of all data and media prior to reassignment Observed Robust Inventory Management and verified that inventory is wiped using DoD standards when devices are reassigned	No Relevant Exceptions Noted
CC6.5.3	Secure shred bins are present in each location that personnel can use to appropriately dispose of any confidential information; all documents in these bins are shredded by a third-party vendor regularly.	Observed the presence of shred bins in each location that can be used to appropriately dispose of any confidential information	No Relevant Exceptions Noted

CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
CC6.6.1	All users that connect to the network resources remotely must use MFA, per the Person or Entity Authentication Policy.	Reviewed the Person or Entity Authentication Policy and verified that all users that connect to the network resources remotely must use MFA Interviewed the Security & Compliance Consultant regarding the use of MFA and verified that all privileged access and remote access requires MFA Observed OpenVPN and verified that users are required to use MFA Observed AWS IAM and verified that all users are required to use MFA	No Relevant Exceptions Noted
CC6.6.2	A firewall is used to prevent and detect any unauthorized traffic or activity on organizational systems and networks.	Interviewed the Security & Compliance Consultant regarding the firewall management of the organization and verified that the facility firewall is managed by Robust Observed Nipper analysis and responses from the organization to determine that the firewall is properly configured and verified that any findings from the Nipper report were false positives	No Relevant Exceptions Noted
CC6.6.3	The application development, production, and staging environments are logically and physically separated using VPCs, separate AWS buckets, and security groups.	Reviewed the Network Connectivity Diagram and verified that the development and staging environments within AWS are on separate VPCs and the production environment is in its own separate AWS account Interviewed the Principal Engineer regarding the production and development environment and verified that the development and staging environments within AWS are on separate VPCs and the production environment is in its own separate AWS account Observed the Software Development Change Management Process and verified that there are separate	No Relevant Exceptions Noted

		accounts for development and production in AWS and are unique and must be accessed separately Observed a sample of the company's production servers (8 of 19) and development and staging servers (7 of 33) and verified that the production servers are housed in a separate AWS account from the development and staging servers	
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		
CC6.7.1	Claritas Rx's encryption requirements and procedures (documented within the Encryption and Decryption Policy) are based on industry-accepted encryption best practices that comply with FIPS 140-2.	Reviewed the Encryption and Decryption Policy and verified that the encryption requirements and procedures are based on industry-accepted encryption best practices, including the following: • NIST SP 800-52 Guidelines for the Selection and Use of TLS Implementations • NIST SP 800-77, Guide to IPsec VPNs • NIST SP 800-113, Guide to SSL VPNs • All sources that are FIPS 140-2 validated Observed AWS resources for organization and verified the use of AWS KMS for organization's key management and encrypted AWS S3 buckets for storage of information	No Relevant Exceptions Noted
CC6.7.2	All data, PHI, and other sensitive information handled by the company is encrypted at rest using 256-bit AES encryption keys, which are managed via AWS's KMS.	Reviewed the Encryption and Decryption Policy and verified that all data, PHI, and other sensitive information handled by the company is encrypted at rest using 256-bit AES encryption keys Interviewed the Principal Engineer and verified that encryption keys are managed via AWS KMS Observed AWS resources for organization and verified the use of	No Relevant Exceptions Noted

		AWS KMS for organization's key management and encrypted AWS S3 buckets for storage of information	
CC6.7.3	All data, PHI, and other sensitive information handled by the company is encrypted in transit via HTTPS and TLS v1.2 or greater where possible, per the Integrity Controls Policy.	Reviewed the Integrity Controls Policy and verified the scope of the policy applies to the organization in its entirety and ensures the integrity of sensitive information in transit by using TLS v1.2 or greater for all transmissions Reviewed the Encryption and Decryption Policy and verified that all data, PHI, and other sensitive information handled by the company is encrypted in transit via HTTPS and TLS v1.2 or greater where possible Observed AWS resources for organization and verified the use of AWS KMS for organization's key management and encrypted AWS S3 buckets for storage of information	No Relevant Exceptions Noted
CC6.7.4	Connections and/or data transfers between Claritas Rx and its customers and third parties are secured using a SSH channel equipped with public/private key authentication and SFTP.	Interviewed the Security & Compliance Consultant, and the Principal Engineer regarding use of SFTP for data transfer communications between organization and its customers and verified that connections and/or data transfers between Claritas Rx and its customers and third parties are secured using a SSH channel equipped with public/private key authentication and SFTP Observed a connection to the organization's SFTP site by the Principal Engineer and verified that connections are secured via authentication using SSH keys	No Relevant Exceptions Noted
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
CC6.8.1	Antivirus and anti-malware programs are implemented on all individual end-user systems and organizational servers and are configured in a manner preventing	Reviewed the Vulnerability Management Policy (dated June 28, 2021) and verified that the organization implements antivirus and	No Relevant Exceptions Noted

	the altering of the programs' settings.	anti-malware programs on individual end-user systems Interviewed the Security & Compliance Consultant and verified that all workstation antivirus and anti-malware is managed using Trend Micro Observed the Trend Micro server and verified the following: • All workstations are updated daily • Local users cannot disable or alter their antivirus settings without an Admin password • Alerts are sent to Robust for investigation upon detection of a virus or issue • Logs document all incidents and issues and are retained for at least one year Observed a sample of workstations (3 of 38) and verified that workstations are equipped with Trend Micro, which performs scans and updates daily, alerts personnel to any detected viruses or issues, and logs any detected issues for forensic analysis Observed a sample of the company's production servers (8 of 19) and development and staging servers (7 of 33) and verified that these servers are equipped with clamscan, an antivirus scanner Observed Ansible and verified that Ansible is used to deploy servers with clamscan; the company uses IaaC and manages the configuration of this infrastructure using Ansible and pre-configured playbooks	
CC6.8.2	The antivirus and anti-malware programs in use performs scans and updates daily, alerts personnel to any detected viruses or issues,	Reviewed the Vulnerability Management Policy and verified that the organization implements antivirus and anti-malware programs on individual end-user systems	No Relevant Exceptions Noted

	and logs any detected issues for forensic analysis.	Interviewed the Security & Compliance Consultant and verified that all workstation antivirus and anti-malware is managed by Robust who uses Trend Micro Observed the Trend Micro server and verified the following: • All workstations are updated daily • Local users cannot disable or alter their antivirus settings without an Admin password • Alerts are sent to Robust for investigation upon detection of a virus or issue • Logs document all incidents and issues and are retained for at least one year Observed a sample of workstations (3 of 38) and verified that workstations are equipped with Trend Micro, which performs scans and updates daily, alerts personnel to any detected viruses or issues, and logs any detected issues for forensic analysis Observed a sample of the company's production servers (8 of 19) and development and staging servers (7 of 33) and verified that these servers are equipped with clamscan, an antivirus scanner Observed Ansible and verified that Ansible is used to deploy servers with clamscan; the company uses IaaC and manages the configuration of this infrastructure using Ansible and pre-configured playbooks	

Trust Services Criteria for the Security and Confidentiality Categories			
System Operations			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		
CC7.1.1	The Vulnerability Management Policy dictates the required monitoring of all organizational systems and devices and the identification and management of detected vulnerabilities.	Reviewed the Vulnerability Management Policy and verified that the performs workstation vulnerability scanning monthly and employs a third party to conduct external penetration tests annually Observed the results of Monthly Nessus Vulnerability Tests and verified that vulnerability scans are conducted of the workstations of the organization and any identified critical or high vulnerabilities are immediately addressed and remediated	No Relevant Exceptions Noted
CC7.1.2	Claritas Rx performs workstation vulnerability scanning monthly and employs a third party to conduct external penetration tests annually.	Reviewed the Vulnerability Management Policy and verified that the company performs workstation vulnerability scanning monthly and employs a third party to conduct external penetration tests annually Observed the results of Monthly Nessus Vulnerability Tests and verified that vulnerability scans are conducted of the workstations of the organization and any identified critical or high vulnerabilities are immediately addressed and remediated	No Relevant Exceptions Noted
CC7.1.3	Claritas Rx performs periodic application vulnerability scanning and employs a third party to perform annual web application tests to test for common vulnerabilities.	Reviewed the Vulnerability Management Policy and verified that the organization performs periodic application vulnerability scanning and employs a third party to perform annual web application tests to test for common vulnerabilities Interviewed the Principal Engineer regarding the application testing and verified that annual web application tests are performed by third parties to test for common vulnerabilities	No Relevant Exceptions Noted

		Observed the results of a Web Application Penetration Test (dated November 22, 2021) and verified that application penetration tests are conducted annually, findings are documented, and any critical or high vulnerabilities are immediately addressed and remediated	
CC7.1.4	Code must be reviewed by at least one other developer during the peer review process to ensure functionality, and QA personnel must approve functionality testing before code is sent to deployment.	Interviewed the Principal Engineer regarding the application testing and verified code must be reviewed by at least one other developer during the peer review process to ensure functionality, and QA personnel must approve functionality testing before code is sent to deployment Observed the Change Management Process and verified that code must complete peer review before it is sent to QA or staging	No Relevant Exceptions Noted
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
CC7.2.1	An intrusion detection systems (IDS) is used that generates alerts upon detection of an intrusion, and these alerts are emailed to Security Engineers for investigation and remediation.	Interviewed the Principal Engineer regarding and verified that Alert Logic is used as an IDS that generates alerts upon detection of an intrusion, and these alerts are emailed to Security Engineers for investigation; Alert Logic also generates logs documenting all detected intrusions and incidents, and all logs are sent to Splunk for retention Observed Alert Logic and verified that Alert Logic is used for IDS; alerts are emailed to Security Engineers and logs are sent to Splunk for retention and any further needed analysis	No Relevant Exceptions Noted
CC7.2.2	The IDS also generates logs documenting all detected intrusions and incidents, and all logs are retained for future review.	Interviewed the Principal Engineer regarding IDS and verified that Alert Logic is used as an IDS that generates alerts upon detection of an intrusion, and these alerts are emailed to Security Engineers for investigation; Alert	No Relevant Exceptions Noted

		Logic also generates logs documenting all detected intrusions and incidents, and all logs are sent to Splunk for retention Observed Alert Logic and verified that Alert Logic is used for IDS; alerts are emailed to Security Engineers and logs are sent to Splunk for retention and any further needed analysis	
CC7.2.3	Network monitoring and logging tools are used to monitor and log the network activity of the organization; these activity logs document all relevant details for all network activity.	Interviewed the Security & Compliance Consultant regarding the network logging and monitoring tools of the organization and verified that AlertLogic and Splunk are used to monitor and log the network activity of the organization; all logs including production server logs and database logs are sent to Splunk, and alerts are sent to the Security Team Observed a sample of the company's production servers (8 of 19) and development and staging servers (7 of 33) and verified that all servers are equipped with Splunk Observed logs generated by Splunk and verified that they document the following details for all network activity: • Source IP • Destination IP • Destination port • Protocol type • Timestamp	No Relevant Exceptions Noted
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		
CC7.3.1	All critical or high vulnerabilities found during penetration tests are entered into a bug tracking system, analyzed and assigned a severity rating, and remediated according to this rating.	Reviewed the Vulnerability Management Policy and verified that all critical or high vulnerabilities found during penetration tests are entered into a bug tracking system, analyzed and assigned a severity rating, and remediated according to this rating	No Relevant Exceptions Noted

		Observed the results of Monthly Nessus Vulnerability Tests and verified that vulnerability scans are conducted of workstations and any identified critical or high vulnerabilities are immediately addressed and remediated	
CC7.3.2	Vulnerabilities assigned a severity of Critical must be mitigated and/or remediated as soon as possible and within a maximum of 30 days after detection.	Reviewed the Vulnerability Management Policy and verified that vulnerabilities assigned a severity of Critical must be mitigated and/or remediated as soon as possible and within a maximum of 30 days after detection Observed the results of Monthly Nessus Vulnerability Tests and verified that vulnerability scans are conducted of workstations and any identified critical or high vulnerabilities are immediately addressed and remediated	No Relevant Exceptions Noted
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
CC7.4.1	The Incident Response Plan outlines the required procedure for handling detected incidents, including activation of the plan and detailed response actions for each organizational department.	Reviewed the Incident Response Plan (dated May 27, 2021) and verified that the plan outlines the required procedure for handling detected incidents, including activation of the plan and detailed response actions for each organizational department Observed a walkthrough of the incident response process and verified that the Breach Evaluation Procedure and the Incident response Plan is used to address detected security breaches and incidents	No Relevant Exceptions Noted
CC7.4.2	The plan describes the roles and responsibilities of the Incident Response Team members and their business units, which include representatives from management, and the Engineering, IT/Operations, Customer Support, HR, Public Relations, and Finance departments.	Reviewed the Incident Response Plan and verified that the plan describes the roles and responsibilities of the Incident Response Team members and their business units, which include representatives from management, and the Engineering, IT/Operations, Customer Support, HR, Public Relations, and Finance departments	No Relevant Exceptions Noted

		Observed a walkthrough of the incident response process and verified that the Breach Evaluation Procedure and the Incident response Plan is used to address detected security breaches and incidents	
CC7.4.3	Formal incident notification and reporting requirements are defined and used by the Incident Response Team to ensure compliance with HIPAA and HITECH.	Reviewed the Incident Response Plan and verified that formal incident notification and reporting requirements are defined and used by the Incident Response Team to ensure compliance with HIPAA and HITECH Observed a walkthrough of the incident response process and verified that the Breach Evaluation Procedure and the Incident response Plan is used to address detected security breaches and incidents	No Relevant Exceptions Noted
CC7.4.4	The Incident Response Team conducts an annual review of the Incident Response Plan, including reviewing team roles and responsibilities, the organization's definition of what constitutes a breach, classification of data, notification requirements, and reporting requirements.	Reviewed the Incident Response Walkthrough (dated August 9, 2021) and verified that the Incident Response Team conducts an annual review of the Incident Response Plan, including reviewing team roles and responsibilities, the organization's definition of what constitutes a breach, classification of data, notification requirements, and reporting requirements Observed a walkthrough of the incident response process and verified that the Breach Evaluation Procedure and the Incident response Plan is used to address detected security breaches and incidents	No Relevant Exceptions Noted
CC7.4.5	All detected incident and security breaches are documented and tracked until remediation using the Breach Investigation Log, which documents a description of the incident or breach, evidence of, any disseminated notifications regarding, and the actions taken to mitigate or remediate the issue.	Reviewed the Breach Investigation Log and verified that all detected incident and security breaches are documented and tracked until remediation using the log, which documents a description of the incident or breach, evidence of, any disseminated notifications regarding, and the actions taken to mitigate or remediate the issue	No Relevant Exceptions Noted

		Observed a walkthrough of the incident response process and verified that the Breach Evaluation Procedure and the Incident response Plan is used to address detected security breaches and incidents	
CC7.4.6	An annual evaluation of all incidents that have been reported, including parties involved, the classification of involved data, the need of notification, and lessons learned following the resolution of the incident is performed; this review is guided by the Breach Evaluation Procedure.	Reviewed the Breach Evaluation Procedure and verified that the organization performs an annual evaluation of all incidents that have been reported, including parties involved, the classification of involved data, the need of notification, and lessons learned following the resolution of the incident Observed a walkthrough of the incident response process and verified that the Breach Evaluation Procedure and the Incident response Plan is used to address detected security breaches and incidents	No Relevant Exceptions Noted
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.		
CC7.5.1	Critical security patches are applied as soon as reasonably possible after release from the vendor, typically no later than the next weekly deployment, as required by the Patching Process.	Reviewed the Patching Process (dated June 29, 2021) and verified that critical security patches are applied as soon as reasonably possible after release from the vendor, typically no later than the next weekly deployment Interviewed the Security & Compliance Consultant regarding the patching of the organization and verified the following: • Servers are patched using Ansible deployments • Workstations are monitored and patched by Robust • Robust supplies monthly Nessus vulnerability scans of all of the workstations to confirm appropriate patching has been completed Observed the company's patching process and verified that critical security patches are applied as soon as reasonably possible after release from	No Relevant Exceptions Noted

		the vendor, typically no later than the next weekly deployment	
CC7.5.2	Patches on production systems may require complex testing and installation procedures, and in certain cases, risk mitigation rather than patching may be preferable.	Reviewed the Patching Process and verified that patches on production systems may require complex testing and installation procedures, and in certain cases, risk mitigation rather than patching may be preferable Interviewed the Security & Compliance Consultant regarding the patching of the organization and verified the following: • Servers are patched using Ansible deployments • Workstations are monitored and patched by Robust • Robust supplies monthly Nessus vulnerability scans of all of the workstations to confirm appropriate patching has been completed Observed the company's patching process and verified that patches on production systems may require complex testing and installation procedures, and in certain cases, risk mitigation rather than patching may be preferable	No Relevant Exceptions Noted
CC7.5.3	A risk assessment is conducted by the Security Officer, and any deviation from required patch implementation timelines is documented and authorized by the Security Officer.	Reviewed the Patching Process and verified that a risk assessment is conducted by the Security Officer, and any deviation from required patch implementation timelines is documented and authorized by the Security Officer Interviewed the Security & Compliance Consultant regarding the patching of the organization and verified the following: • Servers are patched using Ansible deployments • Workstations are monitored and patched by Robust • Robust supplies monthly Nessus vulnerability scans of all of the workstations to confirm	No Relevant Exceptions Noted

		appropriate patching has been completed Observed the company's patching process and verified that a risk assessment is conducted by the Security Officer, and any deviation from required patch implementation timelines is documented and authorized by the Security Officer	

Trust Services Criteria for the Security and Confidentiality Categories			
Change Management			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		
CC8.1.1	The Change Management Policy is used to identify, request, approve, and implement all organizational infrastructure and configuration changes.	Reviewed the Change Management Policy (dated June 2, 2021) and verified that the policy is used to identify, request, approve, and implement all organizational infrastructure and configuration changes Observed the use of Jira to internally manage the communication of change request and change progress alerts and updates	No Relevant Exceptions Noted
CC8.1.2	Change requests must be submitted for approval and implementation by the Product Management and Engineering departments via a change request ticket.	Reviewed the Change Management Policy and verified that change requests must be submitted for approval and implementation by the Product Management and Engineering departments via a change request ticket Interviewed the Security & Compliance Consultant regarding the configuration change management process and verified that all changes are tracked in Jira Observed the use of Jira to internally manage the communication of change request and change progress alerts and updates	No Relevant Exceptions Noted
CC8.1.3	Approved changes are entered into a backlog that is addressed and groomed by the Product Management and Engineering departments.	Reviewed the Change Management Policy and verified that approved changes are entered into a backlog that is addressed and groomed by the Product Management and Engineering departments Interviewed the Security & Compliance Consultant regarding the configuration change management	No Relevant Exceptions Noted

		process and verified that all changes are tracked in Jira Observed the use of Jira to internally manage the communication of change request and change progress alerts and updates	
CC8.1.4	Estimated timelines and implementation tasks and assignments are established by the Engineering department.	Reviewed the Change Management Policy and verified that estimated timelines and implementation tasks and assignments are established by the Engineering department Observed the use of Jira to internally manage the communication of change request and change progress alerts and updates	No Relevant Exceptions Noted
CC8.1.5	All changes must be assessed and approved by the QA department before the change can be implemented.	Reviewed the Change Management Policy and verified that all changes must be assessed and approved by the QA department before the change can be implemented/promoted to the application staging and production environments Observed the use of Jira to internally manage the communication of change request and change progress alerts and updates	No Relevant Exceptions Noted
CC8.1.6	All changes are required to be requested, documented, and tracked to implementation via the use of an internal ticketing system, and these change request tickets document all relevant details regarding the change.	Reviewed 30 infrastructure change tickets and verified that the tickets document the following details for each requested change: • Clearly identified roles and responsibilities • Who authorized and approved the change • What testing was performed prior to the implementation of the change • A defined process for notifying customers prior to changes being made which may impact their service (if applicable) • Post-installation validation processes and their results	No Relevant Exceptions Noted

		• The back-out or recovery plans that were developed for the change Interviewed the Security & Compliance Consultant regarding the configuration change management process and verified that all changes are tracked in Jira Observed the use of Jira to internally manage the communication of change request and change progress alerts and updates	
CC8.1.7	The Change Management Policy is used to identify, request, approve, and implement all application and software development-related changes.	Reviewed the Change Management Policy and verified that policy is used to identify, request, approve, and implement application and software development-related changes Interviewed the Security & Compliance Consultant regarding the configuration change management process and verified that all changes are tracked in Jira Observed the use of Jira to internally manage the communication of change request and change progress alerts and updates	No Relevant Exceptions Noted
CC8.1.8	Change requests for all application and software development-related changes must be submitted for approval and implementation by the Product Management and Engineering departments via a change request ticket.	Reviewed the Change Management Policy and verified that change requests for all application and software development-related changes must be submitted for approval and implementation by the Product Management and Engineering departments via a change request ticket Interviewed the Security & Compliance Consultant regarding the configuration change management process and verified that all changes are tracked in Jira Observed the use of Jira to internally manage the communication of change	No Relevant Exceptions Noted

		request and change progress alerts and updates	
CC8.1.9	Approved software development-related changes are entered into a backlog that is addressed and groomed by the Product Management and Engineering departments.	Reviewed the Change Management Policy and verified that approved software development-related changes are entered into a backlog that is addressed and groomed by the Product Management and Engineering departments Interviewed the Security & Compliance Consultant regarding the configuration change management process and verified that all changes are tracked in Jira Observed the use of Jira to internally manage the communication of change request and change progress alerts and updates	No Relevant Exceptions Noted
CC8.1.10	Estimated timelines and implementation tasks and assignments are established for all application and software development-related changes by the Engineering department.	Reviewed the Change Management Policy and verified that estimated timelines and implementation tasks and assignments are established by the Engineering department Observed the use of Jira to internally manage the communication of change request and change progress alerts and updates	No Relevant Exceptions Noted
CC8.1.11	All application and software development-related changes must be assessed and approved by the QA department before the change can be promoted to the application staging and production environments.	Reviewed the Change Management Policy and verified that all changes must be assessed and approved by the QA department before the change can be implemented/promoted to the application staging and production environments Interviewed the Security & Compliance Consultant regarding the configuration change management process and verified that all changes are tracked in Jira Observed the use of Jira to internally manage the communication of change request and change progress alerts and updates	No Relevant Exceptions Noted

CC8.1.12	During deployment, all code is deployed to a pre-production environment and tested before it is deployed to production; scripts are used to pull down the latest release branch to deploy to the production environment.	Interviewed the VP of Engineering regarding the change control process and verified that during deployment, all code is deployed to a pre-production environment and tested before it is deployed to production; scripts are used to pull down the latest release branch from Bitbucket to deploy to the production environment Interviewed the Security & Compliance Consultant regarding the configuration change management process and verified that all changes are tracked in Jira Observed the use of Jira to internally manage the communication of change request and change progress alerts and updates	No Relevant Exceptions Noted
CC8.1.13	All application and software development-related changes are required to be requested, documented, and tracked to implementation via the use of an internal ticketing system, and these change request tickets document all relevant details regarding the change.	Interviewed the Security & Compliance Consultant regarding the configuration change management process and verified that all changes are tracked in Jira Observed the use of Jira to internally manage the communication of change request and change progress alerts and updates Observed a sample of application and software development-related change request tickets (30 of 423) and verified that the tickets document the following details for each requested change • The subject of the change • A description of the change • Who requested the change • Who approved the change and when • The requested change date • The change's priority rating • The Developer or Team assigned to implement the change • The employee or Team assigned to test the change • Additional assignees, if any	No Relevant Exceptions Noted

		• The change's implementation plan • The change's test plan • The change's rollback and/or rollforward plan	
CC8.1.14	The Configuration Standards, used to configure all organizational systems and devices, are based on the industry-accepted system configuration and hardening best practice NIST SP 800-128 Guide for Security Focused Configuration Management and CIS Benchmarks.	Reviewed the Configuration Standards (dated June 6, 2021) and verified that the company's configuration standards in place are based on the industry-accepted system configuration and hardening best practice NIST SP 800-128 Guide for Security Focused Configuration Management and CIS Benchmarks Interviewed the Security & Compliance Consultant regarding how the organization keeps configuration standards up to date and verified that Standard Amazon Machine Images (AMIs) are used to implement server configuration standards in compliance with CIS standards	No Relevant Exceptions Noted
CC8.1.15	The company uses IaaC and manages the configuration of this infrastructure using Ansible pre-configured playbooks.	Observed Ansible and verified that Ansible is used to deploy servers with clamscan; the company uses IaaC and manages the configuration of this infrastructure using Ansible and pre-configured playbooks	No Relevant Exceptions Noted
CC8.1.16	Standard AMIs are used to implement server configuration standards in compliance with CIS standards.	Interviewed the Security & Compliance Consultant regarding how the organization keeps configuration standards up to date and verified that Standard AMIs are used to implement server configuration standards in compliance with CIS standards Observed Ansible and verified that servers are updated regularly using playbooks that use the latest AMIs, which comply with CIS standards	No Relevant Exceptions Noted
CC8.1.17	The Engineering Team is notified by Amazon whenever there is a new AMI version, and this new image is then incorporated into the Ansible playbooks for deployment.	Interviewed the Security & Compliance Consultant regarding how the organization keeps configuration standards up to date and verified that the Engineering Team is notified by Amazon whenever there is a new AMI version, and this new image is then	No Relevant Exceptions Noted

		incorporated into the Ansible playbooks for deployment Observed Ansible and verified that servers are updated regularly using playbooks that use the latest AMIs, which comply with CIS standards Observed alerts from AWS and verified that the Engineering Team is alerted when a new image version is available for deployment that is built using the latest CIS standards	

Trust Services Criteria for the Security and Confidentiality Categories			
Risk Mitigation			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
CC9.1.1	Claritas Rx considers the risk of potential business disruptions during its annual risk assessment.	Reviewed the Risk Management Plan and verified that the risk assessment process is based on the NIST SP 800-30 and is performed at least annually and after any significant changes to the environment Interviewed the Security & Compliance Consultant regarding the risk management program and verified that Claritas Rx considers the risk of potential business disruptions during its annual risk assessment Observed the Risk Register and verified that the Risk Management Team annually reviews the controls from the risk register that transfer, avoid, and mitigate risk to calibrate their effectiveness and implement adjustments as needed to meet the current needs and threats to the security posture of the organization	No Relevant Exceptions Noted
CC9.2	The entity assesses and manages risks associated with vendors and business partners.		
CC9.2.1	Risk assessments are conducted on all vendors and business partners during the due diligence process.	Reviewed the Risk Management Plan and verified that the risk assessment process is based on NIST SP 800-30 and is performed at least annually and after any significant changes to the environment Interviewed the Security & Compliance Consultant regarding the risk management program and verified that risk assessments are conducted on all vendors and business partners during the due diligence process Observed the Risk Register and verified that the Risk Management Team annually reviews the controls from the risk register that transfer,	No Relevant Exceptions Noted

		avoid, and mitigate risk to calibrate their effectiveness and implement adjustments as needed to meet the current needs and threats to the security posture of the organization	
CC9.2.2	The Vendor Management Procedure outlines required due diligence and ongoing compliance management procedures and standards.	Reviewed the Vendor Management Procedure (dated August 10, 2021) and verified that the policy outlines required due diligence and ongoing compliance management procedures and standards	No Relevant Exceptions Noted
CC9.2.3	Prior to engagement with a third party, the organization completes an in-depth review of the potential vendor's security procedures.	Reviewed the Vendor Management Procedure and verified that the policy outlines required due diligence and ongoing compliance management procedures and standards Interviewed the Security & Compliance Consultant regarding the due diligence performed prior to engaging with a third party and verified that prior to engagement with a third party, the organization completes an in-depth review of the potential vendor's security procedures Observed the company's vendor due diligence process and verified that prior to engagement with a third party, the organization completes an in-depth review of the potential vendor's security procedures	No Relevant Exceptions Noted
CC9.2.4	Potential vendors are required to complete a security questionnaire that is reviewed by the Information Security Team, who completes a Security Risk Assessment to determine if the potential vendor is compliant with the internal policies and standards of Claritas Rx.	Reviewed the Vendor Management Procedure and verified that the policy outlines required due diligence and ongoing compliance management procedures and standards Interviewed the Security & Compliance Consultant regarding the due diligence performed prior to engaging with a third party and verified that potential vendors are required to complete a security questionnaire that is reviewed by the Information Security Team, who completes a Security Risk Assessment to determine if the potential vendor is	No Relevant Exceptions Noted

		compliant with the internal policies and standards of Claritas Rx Observed the company's vendor due diligence process and verified that potential vendors are required to complete a security questionnaire that is reviewed by the Information Security Team, who completes a Security Risk Assessment to determine if the potential vendor is compliant with the internal policies and standards of Claritas Rx	
CC9.2.5	In addition, the potential vendor may be required to provide evidence of any certifications, independent audit reports, or other evidence of a strong security profile, and any potential vendor that would potentially handle PHI or PII on the organizations' behalf must provide a current security certification or audit report (ISO 27001, SOC 2 Type II, HITRUST or equivalent).	Reviewed the Vendor Management Procedure and verified that the policy outlines required due diligence and ongoing compliance management procedures and standards Interviewed the Security & Compliance Consultant regarding the due diligence performed prior to engaging with a third party and verified that the potential vendor may be required to provide evidence of any certifications, independent audit reports, or other evidence of a strong security profile, and any potential vendor that would potentially handle PHI or PII on the organizations' behalf must provide a current security certification or audit report (ISO 27001, SOC 2 Type II, HITRUST or equivalent) Observed the company's vendor due diligence process and verified that a potential vendor may be required to provide evidence of any certifications, independent audit reports, or other evidence of a strong security profile	No Relevant Exceptions Noted
CC9.2.6	Each potential vendor is evaluated based on content provided, customization of the service, ease of use, documented issues, support metrics, and pricing; all information gathered during the due diligence process	Reviewed the Training Vendor Comparison spreadsheet and verified that during the due diligence process for the selection of training system vendors, independent audit reports were obtained and each potential vendor is evaluated based on content provided, customization of the service,	No Relevant Exceptions Noted

	is captured within service-specific comparison spreadsheets.	ease of use, documented issues, support metrics, and pricing; all information gathered during the due diligence process is captured within service-specific comparison spreadsheets Observed the company's vendor due diligence process and verified that vendor service performance is evaluated, including their adherence to defined SLAs, any identified problems in functionality, their impact to Claritas Rx's business functions, and their compliance with applicable regulations and auditing frameworks	
CC9.2.7	Vendor service performance is evaluated, including their adherence to defined SLAs, any identified problems in functionality, their impact to Claritas Rx's business functions, and their compliance with applicable regulations and auditing frameworks.	Reviewed the Vendor Evaluation spreadsheet and verified that the organization monitors service performance including their adherence to defined SLAs, any identified problems in functionality, their impact to Claritas Rx's business functions, and their compliance with applicable regulations and auditing frameworks Observed the company's vendor due diligence process and verified that vendor service performance is evaluated, including their adherence to defined SLAs, any identified problems in functionality, their impact to Claritas Rx's business functions, and their compliance with applicable regulations and auditing frameworks	No Relevant Exceptions Noted
CC9.2.8	An annual review of all third-party service providers and vendors is conducted by requiring the relevant Subject Matter Expert or System Owner to answer several security questions, and the vendor's service delivery and compliance status is determined based on their answers.	Reviewed the Vendor Management Procedure and verified that the policy outlines required due diligence and ongoing compliance management procedures and standards Interviewed the Security & Compliance Consultant and verified that the organization completes an annual review of all third-party service providers and vendors by requiring the relevant Subject Matter Expert or System Owner to answer the following questions, and the vendor's service	No Relevant Exceptions Noted

		delivery and compliance status is determined based on their answers: • Was their downtime beyond expected or outside the range stated in the SLA? • Have there been problems with functionality? • Does the vendor/product still meet our needs? Observed the company's vendor due diligence process and verified that an annual review of all third-party service providers and vendors is conducted by requiring the relevant Subject Matter Expert or System Owner to answer several security questions, and the vendor's service delivery and compliance status is determined based on their answers.	
CC9.2.9	If/when a vendor or third-party service provider has failed to meet Claritas Rx's expectations, replacement of the vendor is considered and discussed by management.	Reviewed the Vendor Management Procedure and verified that the policy outlines required due diligence and ongoing compliance management procedures and standards Interviewed the Security & Compliance Consultant and verified that if/when a vendor or third-party service provider has failed to meet Claritas Rx's expectations, replacement of the vendor is considered and discussed by management Observed the company's vendor due diligence process and verified that if/when a vendor or third-party service provider has failed to meet Claritas Rx's expectations, replacement of the vendor is considered and discussed by management.	No Relevant Exceptions Noted
CC9.2.10	Claritas Rx executes mutual non-disclosure agreements (MNDAs) with its third parties that define the scope of confidential information, requirements and obligations of both parties, the term of the agreement, and the	Reviewed the MNDA (dated December 1, 2021) and verified Claritas Rx executes MNDAs with its third parties that define the scope of confidential information, requirements and obligations of both parties, the term of the agreement, and the	No Relevant Exceptions Noted

	handling of confidential information upon agreement termination.	handling of confidential information upon agreement termination Interviewed the Security & Compliance Consultant and verified the organization requires an executed MNDA prior to sharing confidential information and that MNDAs are managed and tracked via an internal contract management system Observed the company's vendor due diligence process and verified that the organization requires an executed MNDA prior to sharing confidential information and that MNDAs are managed and tracked via an internal contract management system	
CC9.2.11	All executed MNDAs are managed and tracked via an internal contract management system.	Reviewed the MNDA and verified Claritas Rx executes MNDAs with its third parties that define the scope of confidential information, requirements and obligations of both parties, the term of the agreement, and the handling of confidential information upon agreement termination Interviewed the Security & Compliance Consultant and verified the organization requires an executed MNDA prior to sharing confidential information and that MNDAs are managed and tracked via an internal contract management system Observed the company's vendor due diligence process and verified that all executed MNDAs are managed and tracked via an internal contract management system	No Relevant Exceptions Noted

Additional Criteria for Confidentiality			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
C1.1.1	Necessary minimum requirements are in place for handling of sensitive and personal information as required by compliance with HIPAA including when handling PHI internally, when disclosing PHI to an external party in response to a request, and/or when requesting PHI from another covered entity or Business Associate.	Reviewed the Minimum Necessary Policy (dated June 20, 2021) and verified that necessary minimum requirements are in place for handling of sensitive and personal information as required by compliance with HIPAA including when handling PHI internally, when disclosing PHI to an external party in response to a request, and/or when requesting PHI from another covered entity or Business Associate Interviewed the Security & Compliance Consultant and verified that the organization is subject to the elements of the HIPAA Privacy Rule that apply to Business Associates and have implemented policies in regard to the limit of use, disclosure, storage, and disposal of PHI Observed the Privacy Policy published on Claritas Rx's public website and verified that disclosures are in place for the collection, storage, use, and sharing of personal information by the organization's website	No Relevant Exceptions Noted
C1.1.2	These necessary minimum data handling requirements are defined within the formally documented and maintained Minimum Necessary Policy.	Reviewed the Minimum Necessary Policy and verified that necessary minimum requirements are in place for handling of sensitive and personal information as required by compliance with HIPAA including when handling PHI internally, when disclosing PHI to an external party in response to a request, and/or when requesting PHI from another covered entity or Business Associate Observed the Privacy Policy published on Claritas Rx's public website and verified that disclosures are in place for the collection, storage, use, and	No Relevant Exceptions Noted

		sharing of personal information by the organization's website	
C1.1.3	The Data Privacy Officer is responsible for protecting the confidentiality of PHI handled and/or stored by Claritas Rx, and the Data Privacy Officer's roles and responsibilities are formally defined within the Assigned Privacy Responsibility Policy.	Reviewed the Assigned Privacy Responsibility Policy (dated May 28, 2021) and verified that the roles and responsibilities of the Data Privacy Officer are formally defined in regard to protecting the confidentiality of PHI Observed the Privacy Policy published on Claritas Rx's public website and verified that disclosures are in place for the collection, storage, use, and sharing of personal information by the organization's website	No Relevant Exceptions Noted
C1.1.4	A formal Privacy Policy dictating the required disclosures in place for the collection, storage, use, and sharing of personal information by the organization's website is maintained and available for review on the public website.	Observed the Privacy Policy published on Claritas Rx's public website and verified that disclosures are in place for the collection, storage, use, and sharing of personal information by the organization's website	No Relevant Exceptions Noted
C1.1.5	Claritas Rx identifies Confidential information and its responsibilities regarding HIPAA regulations, and procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is required to be retained.	Observed a service delivery walkthrough and verified that the organization identifies Confidential information and its responsibilities regarding HIPAA regulations, and procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is required to be retained	No Relevant Exceptions Noted
C1.1.6	The Data Classification Policy is used to assign all data handled by Claritas Rx a classification that determines the data's handling, processing, encryption, and retention requirement.	Reviewed the Data Classification Policy and verified that this policy is used to assign all data handled by Claritas Rx a classification that determines the data's handling, processing, encryption, and retention requirements; these classifications include the following: • Confidential – Reportable • Confidential • Internal Use Only • Public	No Relevant Exceptions Noted

C1.1.7	Claritas Rx retains all documentation required by the HIPAA regulations for a minimum of six years from the creation date or the date when the document was last in effect, whichever is later.	Reviewed the Documentation Standards and verified that organization retains all documentation required by the HIPAA regulations for a minimum of six years from the creation date or the date when the document was last in effect, whichever is later Interviewed the Security & Compliance Consultant and verified that organization is subject to HIPAA standards for data retention and retains the following data for at least six years from the creation date or last effective date, whichever is later: • Information security and privacy policies and procedures implemented to comply with HIPAA • All documented settings, activities and assessments required by HIPAA • All data use agreements and other forms supporting HIPAA compliance • All signed authorizations and, where applicable, written acknowledgements of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgements • The Notice of Privacy Practices for entities that must provide them • Documentation of the titles of the persons or offices responsible for HIPAA compliance, including not only those with overall responsibility for compliance, but also those responsible for receiving and processing requests for amendments by individuals, and those responsible for receiving and processing requests for an accounting by individuals • Accounting of disclosures of PHI Observed AWS storage and verified that the organization retains all	No Relevant Exceptions Noted

		backups within AWS Glacier for at least six years	
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
C1.2.1	Claritas Rx's data and media erasure and destruction procedures are outlined within the Device and Media Controls Policy, which dictates persistent storage, media re-use, and media disposal requirements and processes.	Reviewed the Device and Media Controls Policy and verified the policy dictates persistent storage, media re-use, and media disposal requirements and processes Observed Robust Inventory Management and verified that inventory is wiped using DoD standards when devices are reassigned Observed the presence of shred bins in each location that can be used to appropriately dispose of any confidential information	No Relevant Exceptions Noted