A-LIGN

A-LIGN.com

Type 2 SOC 2 with HIPAA/HITECH

Prepared for:
Glooko, Inc.

Year:
2026

glooko®
BETTER TOGETHER

REPORT ON GLOOKO, INC.'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY WITH HIPAA/HITECH REQUIREMENTS

Pursuant to Reporting on System and Organization Controls 2 (SOC 2)
Type 2 examination performed under AT-C 105 and AT-C 205

October 1, 2025 to August 31, 2026

Table of Contents

SECTION 1 ASSERTION OF GLOOKO, INC. MANAGEMENT 1

SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT 4

SECTION 3 GLOOKO, INC.'S DESCRIPTION OF ITS ENDOTOOL IV GLUCOSE MANAGEMENT SYSTEM ON PREMISE THROUGHOUT THE PERIOD OCTOBER 1, 2025 TO AUGUST 31, 2026 9

OVERVIEW OF OPERATIONS 10
Company Background 10
Description of Services Provided 10
Principal Service Commitments and System Requirements 10
Components of the System 11
Boundaries of the System 18
RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING 19
Control Environment 19
Risk Assessment Process 20
Information and Communications Systems 21
Monitoring Controls 21
HIPAA/HITECH REQUIREMENTS AND RELATED CONTROLS 22
Policies and Procedures 23
Security Awareness Training 23
Periodic Testing and Evaluation 23
Remediation and Continuous Improvement 24
Incident Response 24
Changes to the System in the Last 11 Months 24
Incidents in the Last 11 Months 24
Trust Services Criteria and HIPAA/HITECH Requirements Not Applicable to the System 25
Subservice Organizations 25
COMPLEMENTARY USER ENTITY CONTROLS 26
TRUST SERVICES CATEGORIES 28
HEALTH INFORMATION SECURITY PROGRAM 29

SECTION 4 TRUST SERVICES CATEGORY, CRITERIA, HIPAA/HITECH REQUIREMENTS, RELATED CONTROLS, AND TESTS OF CONTROLS 31

GUIDANCE REGARDING TRUST SERVICES CATEGORY, CRITERIA, HIPAA/HITECH REQUIREMENTS, RELATED CONTROLS, AND TESTS OF CONTROLS 32
CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION 33
TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY 33
ADMINISTRATIVE SAFEGUARDS 129
PHYSICAL SAFEGUARDS 174
TECHNICAL SAFEGUARDS 181
ORGANIZATIONAL REQUIREMENTS 197
BREACH NOTIFICATION 204

SECTION 5 OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION 224

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS 225

SECTION 1

ASSERTION OF GLOOKO, INC. MANAGEMENT

ASSERTION OF GLOOKO, INC. MANAGEMENT

September 7, 2026

We have prepared the accompanying description of Glooko, Inc.'s ('Glooko' or 'the Company') EndoTool IV Glucose Management System On Premise titled "Glooko, Inc.'s Description of Its EndoTool IV Glucose Management System On Premise throughout the period October 1, 2025 to August 31, 2026" (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 EndoTool IV Glucose Management System On Premise that may be useful when assessing the risks arising from interactions with Glooko's system, particularly information about system controls that Glooko 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 (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*) and essential elements of the Health Insurance Portability and Accountability Act Security Rule of 2003 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), enacted as part of the American Recovery and Reinvestment Act of 2009.

Glooko uses Microsoft Azure ('Azure' or 'subservice organization') to provide cloud hosting services for the Managed Service version of its on Premise solution. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Glooko, to achieve Glooko's service commitments and system requirements based on the applicable trust services criteria and HIPAA/HITECH requirements. The description presents Glooko's controls, the applicable trust services criteria, HIPAA/HITECH requirements, and the types of complementary subservice organization controls assumed in the design of Glooko's controls. The description does not disclose the actual controls at the subservice organization.

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

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

a. the description presents Glooko's EndoTool IV Glucose Management System On Premise that was designed and implemented throughout the period October 1, 2025 to August 31, 2026, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period October 1, 2025 to August 31, 2026, to provide reasonable assurance that Glooko's service commitments and system requirements would be achieved based on the applicable trust services criteria and HIPAA/HITECH requirements, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Glooko's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period October 1, 2025 to August 31, 2026, to provide reasonable assurance that Glooko's service commitments and system requirements were achieved based on the applicable trust services criteria and HIPAA/HITECH requirements, if complementary subservice organization controls and complementary user entity controls assumed in the design of Glooko's controls operated effectively throughout that period.



Benjamin Chang
VP, Security and IT Operations
Glooko, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

A-LIGN

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Glooko, Inc.

Scope

Glooko

We have examined Glooko accompanying description of its EndoTool IV Glucose Management System On Premise titled "Glooko's Description of Its EndoTool IV Glucose Management System On Premise throughout the period October 1, 2025 to August 31, 2026" (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 October 1, 2025 to August 31, 2026, to provide reasonable assurance that Glooko's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (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*). We have also examined the suitability of the design and operating effectiveness of controls to meet essential elements of the Health Insurance Portability and Accountability Act Security Rule of 2003 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), enacted as part of the American Recovery and Reinvestment Act of 2009.

Glooko uses Azure to provide cloud hosting services for the Managed Service version of its on Premise solution. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Glooko, to achieve Glooko's service commitments and system requirements based on the applicable trust services criteria and HIPAA/HITECH requirements. The description presents Glooko's controls, the applicable trust services criteria, HIPAA/HITECH requirements, and the types of complementary subservice organization controls assumed in the design of Glooko's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, 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 Glooko, to achieve Glooko's service commitments and system requirements based on the applicable trust services criteria and HIPAA/HITECH requirements. The description presents Glooko's controls, the applicable trust services criteria, HIPAA/HITECH requirements, and the complementary user entity controls assumed in the design of Glooko'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.

The information included in section 5, "Other Information Provided by Glooko Service Organization That Is Not Covered by the Service Auditor's Report," is presented by Glooko management to provide additional information and is not a part of the description. Information about Glooko's management's response to testing exceptions has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve Glooko's service commitments and system requirements based on the applicable trust services criteria and HIPAA/HITECH requirements.

Service Organization's Responsibilities

Glooko 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 Glooko's service commitments and system requirements were achieved. Glooko has provided the accompanying assertion titled "Assertion of Glooko, Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Glooko 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 HIPAA/HITECH requirements, 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 and HIPAA/HITECH requirements. 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 and HIPAA/HITECH requirements
- 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 and HIPAA/HITECH requirements
- Evaluating the overall presentation of the description

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

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

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 and HIPAA/HITECH requirements. Also, the projection to the future of any conclusions about the suitability of the design and 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 the 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 listed in section 4.

Opinion

In our opinion, in all material respects,

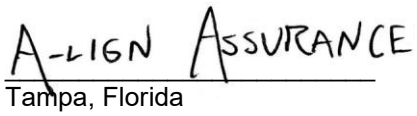
a. the description presents Glooko's EndoTool IV Glucose Management System On Premise that was designed and implemented throughout the period October 1, 2025 to August 31, 2026, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period October 1, 2025 to August 31, 2026, to provide reasonable assurance that Glooko's service commitments and system requirements would be achieved based on the applicable trust services criteria and HIPAA/HITECH requirements, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Glooko's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period October 1, 2025 to August 31, 2026, to provide reasonable assurance that Glooko's service commitments and system requirements were achieved based on the applicable trust services criteria and HIPAA/HITECH requirements, if complementary subservice organization controls and complementary user entity controls assumed in the design of Glooko's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section 4*,* is intended solely for the information and use of Glooko, user entities of Glooko's EndoTool IV Glucose Management System On Premise during some or all of the period October 1, 2025 to August 31, 2026, business partners of Glooko subject to risks arising from interactions with the EndoTool IV Glucose Management System On Premise, 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 and HIPAA/HITECH requirements
- 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.



Tampa, Florida
September 7, 2026

SECTION 3

GLOOKO, INC.'S DESCRIPTION OF ITS ENDOTOOL IV GLUCOSE MANAGEMENT SYSTEM ON PREMISE THROUGHOUT THE PERIOD OCTOBER 1, 2025 TO AUGUST 31, 2026

OVERVIEW OF OPERATIONS

Company Background

Glooko (Monarch) was founded in 2012 with the objective of providing patient-specific insulin dosing software in the United States (US). Monarch has designed and implemented a solution to streamline nursing workflows while prioritizing patient safety. In 2025, Monarch was acquired by Glooko, Inc. to expand Glooko's connected care capabilities into inpatient glycemic management.

Description of Services Provided

With the Monarch acquisition, Glooko's EndoTool Insulin Dosing Software Platform is an electronic Glucose Management System (eGMS) based on a proprietary, patient-personalized algorithm that generates precision insulin dosing recommendations for hospital nurses much more accurately, faster, and safer than any other electronic or paper-based protocol, which significantly improves patient outcomes.

EndoTool is a proprietary technology that uses algorithms to model, predict, and adapt dosing to each patient's physiology and individual response providing insulin dose recommendations for intravenous and subcutaneous delivery.

EndoTool Glycemic Management Software consists of EndoTool IV and EndoTool SubQ which are standalone software classified as Software-as-a-Medical Device by the Food and Drug Administration. EndoTool is a web-based application that can be deployed on-premises.

EndoTool is a glucose management software system used by healthcare professionals in all inpatient care settings for adult and pediatric patients aged two years and above who weigh 12 kgs. or more. EndoTool adjusts and maintains a patient's glucose level within a configurable clinician-determined target range by recommending patient-specific intravenous insulin dosing, carbohydrate dosing for recovery or supplementation, and subcutaneous dosing for the transition from IV dosing.

EndoTool logic is not a substitute for, but rather an adjunct to, clinical reasoning. No medical decision should be based solely on the recommended guidance provided by this software system.

Principal Service Commitments and System Requirements

Glooko designs its processes and procedures related to EndoTool to meet its objectives for its cloud hosted software solutions. Those objectives are based on the service commitments that Glooko makes to user entities, the laws and regulations that govern the provision of its cloud hosted software solutions, and the financial, operational, and compliance requirements that Glooko has established for the services. The cloud hosted software solutions of Glooko are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act Administrative Simplification, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which Glooko operates.

Security commitments to user entities are documented and communicated in the EndoTool Cyber Security Labeling, Service Level Agreements (SLAs) and other customer agreements. Commitments are standardized and include, but are not limited to, the following:

Security principles within the fundamental designs of the EndoTool Software that are designed to permit system users to access the information based on their role in the system while restricting them from accessing information not needed for their role.

Use of encryption technologies to protect customer data both at rest and in transit is implemented. The encryption technologies and methods utilized are defined in the encryption policies and procedures. Critical data including personal information and passwords is required to be stored in an encrypted format. In addition, where employees utilize mobile devices (i.e., phones, laptops, etc.) to access the in-scope systems, the connection must be established in a secure manner using encryption.

Glooko establishes operational requirements that support the achievement of security commitments, service levels, relevant laws and regulations, and other system requirements. Such requirements are communicated in Glooko' system policies and procedures, system design documentation, and contracts and SLAs with customers, vendors and third-parties. Changes to commitments, requirements, and responsibilities are communicated to external parties, including impacted customers and vendors.

Organizational and information security policies are formally documented to support the functioning of internal controls and processes and define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the EndoTool Software. Glooko ensures that the company's organizational and information security policies and procedures are made available to its personnel.

Components of the System

Infrastructure

Primary infrastructure used to provide Glooko' EndoTool IV Glucose Management System On Premise includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Windows Server	2016 or later	Host data
Azure	Cloud Hosting Service	Host virtual servers to support applications and IT operations
.NET Framework	4.8	Application Development Framework
Structured query Language (SQL) Server	MS Server 2019	Database Structure
Active Directory	Microsoft Service	Domain Connection for resource management
Adobe Acrobat	Reader	PDF Reader

Software

Primary software used to provide Glooko' EndoTool IV Glucose Management System On Premise includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Azure Dev Ops	Microsoft Windows	Virtualizing customer networks and host application server virtual machines
Azure Virtual Machines	Microsoft Windows	Host application server virtual machines

Primary Software		
Software	**Operating System**	**Purpose**
Azure App Insights/Azure Monitoring	Software as a Service (SaaS)	Network monitoring and inventory
SecureLink	SaaS	Secure connection to the customer network for installation, maintenance, and support purposes
SQL Server	Windows	Used for EndoTool storage
PostgreSQL	Windows	Used by Mirth Connect for storing configuration and messages that are being processed
Azure Dev Ops	Windows	Ticketing System, Source Code Control, Continuous Integration/Continuous Delivery (CI/CD) pipelines
Windows 10+	Windows	Workstations
Office 365	Cloud	Business Communications
Snyk	SaaS	Vulnerability Scanning
Bamboo Human Resource (HR)	Cloud	Human Resource Management System (HRMS)
Salesforce	Customer Relationship Management (CRM)	Customer Relationship Management Tool

People

Glooko has a staff organized in the following functional areas:

- Corporate Executives, senior operations staff, and company administrative support staff, such as regulatory compliance, finance, human resources, business operations, technology, hospital solutions and clinical provider relations. These individuals use the established quality management system utilized for the manufacture of EndoTool primarily as a tool to measure performance at an overall corporate level. This includes reporting done for internal metrics as well as for Glooko' user entities.
- Technical Support Engineers (TSE) take phone calls directly from customers to provide customers with support as needed for troubleshooting EndoTool. Led the areas of technical support for both internal and external clients, deployment process improvement, and technical design efforts for existing and newly developed products across the Glooko customer and prospect base.
- The Customer Success Manager (CSM) has primary responsibility for managing customer-facing activities to optimize patient outcomes, maximize the utilization of Glooko's software, and support client success. The key activities of this role are as follows: Nurture collegial relationships with providers, nurses, pharmacy, informatics, and administrators within assigned hospitals/hospital systems, facilitate the development of clinical champions within customer hospitals, and conduct quarterly touch points, including business reviews, metrics analysis, case reviews and product feedback with assigned hospitals/hospital systems.
- Clinical Services Specialists (CSS) are the clinical liaison responsible for the successful completion of new customer implementations and current customer upgrades for the entire Glooko product portfolio. This role includes providing user training to customer staff and support through the go-live process, either on-site or virtually. This role will also provide customer insight and clinical expertise to the product management team through direct participation in the product development process.
- Regulatory Affairs monitor for compliance with internal policies and procedures, including HIPAA. Manage complaints and work with the TSE to drive to resolution.

- The Project Implementation Team manages the installation of the EndoTool software within the customer environment by leading a team of TSE's, CSM's, and CSS'.
- Chief Finance Officer (CFO) manages the accounts payable and accounts receivable including the invoices for the customer contracts executed.
- Marketing is responsible for developing and implementing marketing strategies to increase brand awareness, drive user adoption, and support the overall growth of EndoTool.
- Product Managers**:** Glooko' product managers demonstrate and share knowledge and a deep understanding of EndoTool, the competitor's products, as well as the industry and regulatory environment. Contribute to Glooko product roadmap development and lead projects as needed to define new features/functions. Also, assist Software Development with product development efforts including prototyping, troubleshooting complex problems, and providing acceptable solutions. Guide, develop, and/or support messaging, literature, and data reviews in order to support the sales effort and to increase awareness of the product and the clinical problem it addresses. Additionally, provide guidance for customer implementation and training in Glooko products.
- Software Engineering and Development Team has the accountability for ensuring EndoTool products include their intended requirements. These people will help ensure that all the software has been successfully tested prior to its release. This role is responsible for obtaining design help if/when necessary. Assist in the design and documentation of product releases, including system requirements and DHF artifacts. The Glooko Software Engineering and Development Team will assist in installations/upgrades and customer support on technical issues as necessary. Drive improvements within Glooko, assisting with the identification and implementation of process improvements and tool changes.
- Hospital Solutions: The Hospital Solutions Team is responsible for performing a variety of tasks across the sales spectrum including building and communicating the EndoTool brand with target customers and users, building a pipeline of qualified leads, and serving as the business owner and power user of Salesforce.com implementation for sales and marketing.
- IT: IT Help desk, IT infrastructure, IT networking, IT system administration, software systems development and application support, information security, and IT operations personnel manage electronic interfaces and business implementation support and telecom.
    - The help desk group provides technical assistance to the Glooko users.
    - The infrastructure, networking, and systems administration staff typically have no direct use of EndoTool. Rather, it supports Glooko' IT infrastructure, which is used by the software. A Software Development Engineer will deploy the releases of EndoTool and other software into the production environment.
    - The software development staff develops and maintains the custom software for Glooko. This includes EndoTool, supporting utilities, and the external websites that interact with EndoTool. The staff include software developers, software engineers, and software quality assurance.
    - The information security staff supports EndoTool indirectly by monitoring internal and external security threats and maintaining current antivirus software.
    - The information security staff maintains the inventory of IT assets.
    - Software development and DevOps staff manage the hosting infrastructure for EndoTool. This includes Azure Server setup, access, and maintenance including backups.
    - IT third-party Service Provider provides user support to Glooko. This group does not directly use EndoTool, but it provides infrastructure support as well as disaster recovery assistance.

Data

Data, as defined by Glooko, constitutes the following:

- Audit Log
- Transaction data
- Electronic interface files
- Output reports
- Input reports

- System files
- Error logs

The audit log captures and records key activities and events, including the start and end of user sessions, web browser identification, and login attempts. It tracks specific actions such as Active Directory searches, patient enrollment steps, access to patient records, and entry of patient data. Additionally, it logs critical processes like dose calculations, saving downtime reports, and the exit from patient records. Security-related events such as system errors, data validation failures, and the expiration of patient lockout times are also documented, providing a comprehensive record of user interactions and system responses.

Data classification policies and procedures are formally established to define the criticality of the data, data classification schemes, who can access what data, how data is secured, how long data should be retained, and how/when it is purged or destroyed. Data must be classified and structured in a consistent manner. As data is no longer required for business purposes, it is appropriately purged or destroyed. Where there is electronic Protected Health Information (ePHI) data on a device or media that is no longer required, the Company ensures to sanitize the ePHI data prior to the device or media being re-used. Appropriate internal controls have been implemented to protect confidential documents, files, or directories from inappropriate access. In addition, access to confidential and/or customer data is restricted to authorized personnel based on job role and responsibilities.

Management has defined and documented the components of the data critical to supporting the in-scope system including a description of what the critical data is and is used for, the source of the data, and how the data is stored and transmitted.

Operational personnel review data input, processed, and output from the in-scope system for completeness, accuracy, and timeliness. Errors in the processing of critical data are detected, investigated, and resolved in a timely manner.

As data is entered into the in-scope systems, edit checks are in place to help prevent incomplete or incorrect data from being entered in. In addition, the company has documented and maintains data flow diagrams, process flowcharts, narratives and procedures manuals to identify the relevant internal and external information sources of the system as well as how data moves within the environment.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. Logical access includes system settings and configurations, password requirements, access management, authentication, and system and access logging requirements.

Information Security Management System Manual outlines how Glooko uses the appropriate safeguards to ensure the Confidentiality, Integrity, and Availability (CIA) of information assets by protecting those assets from threats, hazards, and unauthorized access, modification, destruction, or disclosure. This includes protected health information that is created, received, maintained, or transmitted by Glooko.

All teams are expected to adhere to Glooko' policies and procedures that define how services should be delivered. These are located in Greenlight Guru and can be accessed by any Glooko team member.

Physical Security

Glooko relies on Azure for cloud hosting services to support their infrastructure and systems for the Managed Service version of its on Premise solution. Refer to the "Subservice Organizations" section below for physical security controls implemented and operated by Azure.

Logical Access

Glooko uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. Privileged access to the in-scope environment (including access to ePHI) is restricted to authorized and appropriate personnel and formally reviewed at least annually. User activity is configured to be logged on to the in-scope systems, and those logs are retained and reviewed as needed.

In the event incompatible responsibilities cannot be segregated, Glooko implements monitoring of one or more of the responsibilities. Monitoring must be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing reviews of access by role.

Employees sign on to the in-scope systems (including those handling or storing ePHI) using a valid user ID and password. Users are required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Active Directory. Passwords must conform to defined password standards and are enforced through parameter settings within the in-scope system. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Customers' employees' access EndoTool through the Internet using the Transport Layer Security (TLS) functionality of their web-browser. These customer employees must supply a valid user ID and password to gain access to customer cloud resources. Passwords must conform to password configuration requirements configured on the virtual devices using the virtual server administration account. Virtual devices are initially configured in accordance with Glooko' configuration standards, but these configuration parameters may be changed by the virtual server administration account.

Customer employees may sign up to their systems using virtual server administration accounts. These administration accounts use a two-factor digital certificate-based authentication system.

Upon hire, employees are assigned to a position in the HR management system. Two days prior to the employees' start date, a software access request form is generated for the new employee by the hiring manager. The form is used by the IT help desk and system administrators to create user IDs and access rules. Access rules have been pre-defined based on the defined roles. The software access form is also used for employees' position changes and the associated roles to be changed within the access rules.

On an annual basis, access rules for each role are reviewed by a working group composed of the information security officer, regulatory affairs and HR personnel. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access. As part of this process, management reviews access by privileged roles and requests modifications based on this review.

The HR system generates a task to remove access for terminated employees upon termination. These tasks are used by the IT help desk and system administrators to delete employee access. Glooko's system administrators review HR systems and active contractor lists quarterly to suspend user IDs and delete all access roles from IDs belonging to terminated employees.

User entities hosting EndoTool within their own infrastructure and environment, have a responsibility to implement logical access controls. Please refer to the "Complementary User Entity Controls" section below for logical access related controls implemented and operated by user entities.

Computer Operations - Backups

The Company has established formal data backup policies and procedures outlining the data backup process, including how and when critical data is backed up. Both critical internal as well as customer data is backed up and monitored by operations personnel for completion and exceptions. In the event of backup failure, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job depending on customer indicated preference within the documented work instructions.

Glooko uses Azure Recovery Services vault which is a management entity that stores recovery points that are created over time and provides an interface to perform backup-related operations. It also provides Glooko with a storage replication option to replicate it to geo-redundant storage, local redundant storage, or zone-redundant storage. Based on customer requirements an appropriate replication mechanism is chosen. Data backup policies and procedures outlining the data backup process, including how and when critical data is backed up is configured within the Backup policies. Azure Recovery Services provides the Company with the option to take on-demand backups and perform restores as needed. Azure alerts are configured to notify the Operations Team to troubleshoot any backup related issues. Data backup and recovery tests are performed annually to ensure business continuity in case of a disaster.

User entities hosting the EndoTool within their own infrastructure and environment, have a responsibility to implement backup related controls for data storage. Please refer to the “Complementary User Entity Controls” section below for backup related controls implemented and operated by user entities.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, document, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents within the in-scope environment. Incidents must be analyzed, classified, prioritized, documented, tracked, investigated, and addressed timely. The status, remediation efforts, resolution of incidents are communicated to affected users. All incidents, including HIPAA-related ones, are documented and tracked using incident management software.

Glooko monitors the capacity utilization and system performance of computing infrastructure, both internally and for Glooko hosting customers, to ensure that service delivery matches SLAs. The monitoring tools are configured to send alerts when capacity utilization or system performance dip below the established thresholds. Alerts are investigated and resolved by support personnel.

Processing capacity and system performance are monitored 24x7x365. Glooko evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Disk storage
- Memory utilization
- Network bandwidth

Glooko has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and Glooko system owners review proposed operating system patches to determine whether the patches are applied. Customers and Glooko systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Glooko staff evaluate that all patches have been installed and if applicable that reboots have been completed.

Glooko has established formal business continuity and disaster recovery plans. These plans are tested at least annually with revisions made to the plans based on the testing results.

User entities hosting EndoTool within their own infrastructure and environment, have a responsibility to implement incident management and business continuity / disaster recovery controls. Please refer to the "Complementary User Entity Controls" section below for incident management and business continuity / disaster recovery related controls implemented and operated by user entities.

Change Control

Glooko maintains documented change management policies and procedures to guide personnel in documenting and implementing system (e.g. application, infrastructure, network, etc.) changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures. The change control procedures also outline the process to follow for emergency changes.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system. Access to promote changes to the production environment is restricted to authorized personnel requiring such access for their role and responsibilities.

Releases are approved by a Change Advisory Board and packed for distribution in a secure location. Changes promoted to the production environment are approved by customers prior to implementation.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Glooko has implemented a patch management process to ensure EndoTool systems are patched in accordance with recommended system patches. Customers and Glooko system owners review proposed operating system patches to determine whether the patches are applied. Customers and Glooko are collectively responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Customers and Glooko staff validate that all patches have been installed and if applicable that reboots have been completed.

Changes made to in-scope systems are communicated to both internal and external users that are affected by the given change.

User entities hosting EndoTool within their own infrastructure and environment, have a responsibility to implement change management controls. Please refer to the "Complementary User Entity Controls" section below for change management related controls implemented and operated by user entities.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Antivirus endpoint protection software is installed on the in-scope production servers and workstations, which is configured to run scans and push updates regularly. The firewall systems and antivirus protection are configured according to the anti-malware and firewall policies and procedures.

An intrusion detection system (IDS) are in-place to prevent and detect unusual activity. The IDS systems are configured to send alerts when potential threats or unusual system activity are detected. Alerts are investigated and resolved by support personnel.

Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Networks and customer environments are segmented logically from each other using VLANs to restrict access.

Glooko monitors the in-scope systems to identify potential security threats and vulnerabilities and to detect unusual system activity. The monitoring tools are configured to send alerts when potential threats or unusual system activity are detected. Alerts are investigated and resolved by support personnel.

The Company has formally defined policies and procedures in place regarding completing penetration tests and vulnerability scans and addressing and remediating identified vulnerabilities.

Penetration testing is conducted annually to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Glooko. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by a third-party vendor during Penetration Testing and by Glooko in accordance with Glooko policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by Glooko. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. To ensure robust security, Glooko conducts weekly Snyk scans that leverage the OWASP and NVS databases to detect vulnerabilities. During the software development process, OWASP Zap Scans are performed at code freeze to identify and address any issues prior to software release. Scans are performed during non-peak windows.

Vulnerabilities identified from the penetration tests and vulnerability scans performed are formally documented, prioritized, addressed and remediate in a timely manner and in accordance with company policies and procedures.

Authorized employees may access SaaS-based tools over the Internet using single sign-on (where available) and access to server infrastructure is via a Bastion host. Employees are authenticated through the use of a token-based two-factor authentication system. User activity is configured to be logged via built-in monitoring tools, and those logs are retained and reviewed as needed. Privileged access to the cloud environment is restricted to authorized personnel requiring such access for their role and responsibilities.

User entities hosting EndoTool within their own infrastructure and environment, have a responsibility to implement data security and internal assessment controls. Please refer to the "Complementary User Entity Controls" section below for data security and internal assessment related controls implemented and operated by user entities.

Boundaries of the System

The scope of this report includes the Glooko' EndoTool IV Glucose Management System On Premise hosted in the Azure infrastructure and administered remotely by Glooko personnel.

This report does not include the cloud hosting services provided by Azure at multiple facilities.

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

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Glooko' control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Glooko' ethical and behavioral standards, how the products are communicated and reinforced in practices. Also, include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. Also, include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees to sign an acknowledgment form and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.
- Employees, third-parties, and customers are informed of how to report unethical behavior in a confidential manner.

Commitment to Competence

Glooko' management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- As part of the hiring process, management evaluates a candidate's competencies, skillsets, and prior experience.
- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Security awareness, HIPAA for Business Associates and Good Manufacturing Practices training is provided at least annually to maintain the knowledge of responsibilities of all personnel of critical processes.

Management's Philosophy and Operating Style

Glooko' management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Management is briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole.

Organizational Structure and Assignment of Authority and Responsibility

Glooko' organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Glooko' assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what will be held accountable. Job descriptions (including for Executive Management) are formally documented and communicated to employees, and management reviews the written job descriptions at least annually for accuracy.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.
- Organizational charts are reviewed for accuracy at least annually by management.

Human Resources Policies and Practices

Glooko' success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Glooko' human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

Risk Assessment Process

Glooko risk assessment process identifies and manages risks that could potentially affect Glooko' ability to provide reliable services to user organizations. This process requires that management identify significant risks inherent in products or services as it oversees their areas of responsibility. Glooko identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by Glooko and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel.
- Strategic risk - new technologies, changing business models, and shifts within the industry.
- Compliance - legal and regulatory changes.

Glooko has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Glooko attempts to actively identify and mitigate significant risks through the implementation of various initiatives and communication with other leadership committees and senior management.

Management has established formal risk assessment policies and procedures which state that a formal risk assessment must be completed at least annually and include an identification and review of risks relating to fraud, vendors and third-parties, and changes to the environment (i.e., people, processes, technologies).

In addition, Glooko performs appropriate due diligence procedures to verify that each vendor and third-parties environment is secure. Where control gaps are identified, Glooko works with the vendor to address and remediate.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Glooko' EndoTool system; as well as the nature of the components of the system result in risks that the criteria will not be met. Glooko addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Glooko' management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication are an integral component of Glooko' internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Glooko information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, Meetings are held annually in a geographic central location to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Glooko personnel via e-mail messages.

Monitoring Controls

Management monitors controls to ensure that operation is as intended and that controls are modified as conditions change. Glooko' management performs monitoring activities to assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through monitoring activities, separate evaluations, or a combination of the two.

Management also maintains a formal internal controls program that describes the implemented internal controls, who is responsible for performing each control, the frequency each control operates, the control type, and how the control is executed. In addition, management meets annually to assess the effectiveness and performance of internal controls within the environment. Executive management maintains independence from those that operate the key internal controls within the environment.

User entities hosting EndoTool within their own infrastructure and environment, have a responsibility to implement monitoring controls. Please refer to the "Complementary User Entity Controls" section below for monitoring related controls implemented and operated by user entities.

On-Going Monitoring

Glooko' management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications. In addition, Glooko has assigned formal responsibility for coordinating and monitoring the compliance and audit activities to ensure the internal controls environment is formally evaluated at least annually through internal audit.

Management's close involvement in Glooko' operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision to address any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Glooko' personnel.

Reporting Deficiencies

A Risk Management Report is utilized to document and track the results of on-going monitoring procedures. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within Greenlight Guru. Annual Management Reviews are held for management to review reported deficiencies and corrective actions.

HIPAA/HITECH REQUIREMENTS AND RELATED CONTROLS

Periodic Assessments

Glooko has a risk assessment process in place to identify and manage the risks that could affect the Company's ability to provide services to its user entities. The risk assessment procedure defines the responsibility, methodologies and processes used by Glooko to assess the risks while providing services and develop mitigation strategies to address those risks. This process requires the Company to identify risk based on management's internal knowledge of its operations. The following risk factors are discussed among the executive management including the Chief Executive Officer (CEO), Chief Medical Officer (CMO) and Chief Fiscal Officer (CFO) at least annually:

- Risk Assessment: The risk assessment is performed by the risk management personnel. Risk factors associated with the delivery or implementation of services to customers are evaluated considering process owners, dependencies, timelines and quality.
- Health Information Security Risks: Health information security risks are assessed by the Information Security Officer or designee and Regulatory Affairs (HIPAA Compliance Officer). Risk factors associated with the organization are evaluated considering compliance obligations, laws and regulations, policies and procedures, contracts and practices to which the organization has committed to. Information security assessments carried out by risk management personnel are rolled up to the CEO, CMO and CFO of the organization.

Policies and Procedures

Glooko has formally documented procedures in place that specify the proper functions, processes, and appropriate environments of workstations that access ePHI. Health information security policies and procedures have been implemented regarding the protection of information assets. The policies and procedures act as a guide for all Glooko personnel. These policies and procedures define guidelines for the health information security program related to scope of services, which includes implementing and managing logical access security and controls, including the following:

- Health information security policy
- Asset management
- Data classification
- Business continuity
- Incident management (including breach handling and notification)
- Access control
- Authentication and authorization of access to ePHI
- Defining, identifying and designating information as PHI or ePHI
- Storing PHI and ePHI
- The mechanisms used to encrypt ePHI data
- Protecting PHI and ePHI from improper alteration, erasure or destruction
- Retaining PHI and ePHI for only as long as is required to achieve the purpose for which the data was collected and processed or a minimum of 6 years
- Maintaining records of the movements of hardware and electronic media
- Requirements from applicable legislation, regulators, and customers

Management has formally documented and assigned to a job role the responsibility for the development, implementation, and regular maintenance of the policies and procedures that govern the security of protected ePHI formally documented and assigned to a job role. The Company's policies and procedures are created and maintained in both written and electronic form.

All teams are expected to adhere to the Glooko policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Glooko' Glooko team member.

The Company's policies and procedures are reviewed and approved by management on at least an annual basis. ePHI-related policies and procedures are retained for a minimum of six (6) years from the date it was created or when it was last in effect, whichever is later. Users are made aware of security updates and updates to security policies and procedures.

Security Awareness Training

Glooko employees receive security awareness training for health information security as part of the onboarding process. This training is reinforced by security awareness communications on current issues. Additionally, employees are also required to participate in annual security awareness training.

Periodic Testing and Evaluation

Glooko completes evaluations throughout each calendar year regarding the effectiveness of the health information security program that includes, but are not limited to, the following:

- Internal risk assessments
- Corrective action plans
- Management reviews

Remediation and Continuous Improvement

Areas of non-compliance in Glooko' internal control system surface from many sources, including the Company's monitoring procedures, separate evaluations of the internal control system, and external parties. Management has developed protocols to help ensure findings, if identified, of internal control, non-compliant items should be reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to areas of non-compliance in internal control procedures and makes the decision to address any non-compliant items based on whether the incident was isolated or requires a change in the Company's procedures or personnel.

Incident Response

Glooko maintains a documented incident response plan including breach notification requirements as mandated by HITECH. The procedures include, but are not limited to, the identification, response, escalation, and remediation of security breaches and other incidents. A formal breach notification process is utilized to document and track resolution of incidents noted. The incident response procedures are tested during the normal course of business and are updated as needed.

Breach Notification

The Company acknowledges responsibility for notifying affected parties in the event of a breach of unsecured protected health information. Breach notification letters or e-mails are formally developed and prepared to be used during a breach of ePHI. The breach notification letter or e-mail template includes the following:

- Notice to parties alerting them to breaches "without unreasonable delay," but no later than 60 days after discovery of the breach.
- Notice covered entities when breach is discovered.
- Notice to the secretary of Health and Human Services (HHS) and prominent media outlets about breaches involving more than 500 individual subjects 'records.
- Notice to next of kind about breaches involving parties who are deceased.
- Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity's response.
- Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches involving fewer than 500 patient records during a breach of ePHI.

Affected parties are notified of a breach of ePHI no later than sixty (60) calendar days after the discovery of the breach, The identification of each individual who's unsecured ePHI has been accessed during the breach is disclosed during notification procedures.

Management provides covered entities with any information that the covered entities are required to include in the notification to the individual at the time of the breach and as soon as it is available. The Company refrains from delays notifying HHS personnel, the covered entity, or other required people following the discovery of a breach of unsecured protected health information when required by law.

Changes to the System in the Last 11 Months

No significant changes have occurred to the services provided to user entities in the 11 months preceding the end of the review period.

Incidents in the Last 11 Months

No significant incidents have occurred to the services provided to user entities in the 11 months preceding the end of the review period.

Trust Services Criteria and HIPAA/HITECH Requirements Not Applicable to the System

All Common/Security criteria were applicable to Glooko' EndoTool IV Glucose Management System On Premise.

The following HIPAA/HITECH requirements were not applicable to the system:

HIPAA/HITECH Requirements Not Applicable to the System		
Safeguard	**Requirement**	**Reason**
Administrative Safeguards	164.308(a)(4)(ii)(A)	The entity is not a healthcare clearinghouse.
	164.308(b)(1)	The entity is not a covered entity.
	164.308(b)(2)	The entity does not use subcontractors. The organization would not share ePHI if it were in their possession.
Physical Safeguards	164.310(c)	The entity is not a covered entity.
Organizational Safeguards	164.314(a)(2)(ii)	The entity is not a government entity.
	164.314(b)(1)	The entity is not a health plan sponsor.
	164.314(b)(2)	The entity is not a group health plan.
reach Safeguard	164.404(a)(1), 164.404(a)(2), 164.404(b), 164.404(c)(1), 164.404(c)(2), 164.404(d)(1)(i), 164.404(d)(1)(ii), 164.404(d)(2), 164.404(d)(2)(i), 164.404(d)(2)(ii), 164.404(d)(3), 164.406, 164.408(a), 164.408(b), 164.408(c)	The entity is a business associate; its responsibilities for breach of notification are limited to its covered entity customers.

Subservice Organizations

This report does not include the cloud hosting services provided by Azure at the multiple facilities.

Subservice Description of Services

Glooko relies on Azure for cloud hosting services to support their in-scope systems and file sharing for the Managed Service version of its on Premise solution.

Complementary Subservice Organization Controls

Glooko' services are designed with the assumption that certain controls will be implemented by the subservice organization. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria and HIPAA/HITECH requirements related to Glooko' services to be solely achieved by Glooko control procedures. Accordingly, the subservice organization, in conjunction with the services, should establish their own internal controls or procedures to complement those of Glooko.

The following subservice organization controls should be implemented by Azure to provide additional assurance that the trust services criteria and HIPAA/HITECH requirements described within this report are met:

Subservice Organization - Azure		
Category	**Criteria/ Regulation**	**Control**
Security / Physical Safeguards	CC6.4, CC7.2, 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310 (d)(1), 164.310 (d)(2)(iii)	Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors.
		Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors.
		Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		The datacenter facility is monitored 24x7 by security personnel.

Glooko management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as SLAs. In addition, Glooko performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports on services provided by vendors and the subservice organization.
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization.

COMPLEMENTARY USER ENTITY CONTROLS

Glooko services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria and HIPAA/HITECH requirements related to Glooko services to be solely achieved by Glooko control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Glooko.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria and HIPAA/HITECH requirements described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Glooko.
2. User entities are responsible for notifying Glooko of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring supervision, management, and control of the use of Glooko services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Glooko services.
6. User entities are responsible for providing Glooko with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Glooko of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
8. User entities are responsible for restricting access to system resources to appropriate user entity personnel.
9. User entities are responsible for performing user access reviews (as defined by policy and compliance requirements) to validate user accounts, including third-party or vendor accounts, and their associated privileges remain appropriate.
10. User entities are responsible for monitoring production systems and resources and alerts are sent out by personnel based on pre-configured rules.
11. User entities are responsible for utilizing a centralized system that collects and stores logs of system activity and sends alerts to personnel based on pre-configured rules.
12. User entities are responsible for the implementation of technical measures to protect stored user passwords for the system (e.g., encryption, hashing, salting, etc.).
13. User entities are responsible for managing access to make changes in production environments and restricting the same to authorized personnel in accordance with segregation of duties principles and the company's documented policies and procedures.
14. User entities are responsible for enabling file integrity monitoring or a change-detection mechanism to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts.
15. User entities are responsible for making changes to system components in the production environment (including software, code, infrastructure, network, configuration changes, etc.) according to established procedures that include documentation (change description, justification, evaluation of security requirements and impact, approval by authorized parties, rollback procedures, etc.) and testing (including acceptance and security impact testing).
16. User entities are responsible for communicating system changes via release notes or changing log in to the company's website.
17. User entities are responsible for peer-review and approval of changes prior to deployment by an individual different from the developer to maintain segregation of duties.
18. User entities are responsible for testing changes in an environment separate from production prior to deployment in accordance with the nature of the change.
19. User entities are responsible for documenting change control policies and procedures to guide personnel in implementing changes in an emergency.

20. User entities are responsible for conducting vulnerability scans of the production environment as dictated by company policy and compliance requirements and the results are reviewed by company personnel and vulnerabilities are tracked to resolution in accordance with company policies.
21. User entities are responsible for managing access to production systems through an encrypted connection (e.g., encrypted virtual private network, etc.)
22. User entities are responsible for configuring the network security to limit inbound and outbound traffic to the environment to only what is necessary based on business justification.
23. User entities are responsible for implementing an IDS to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected.
24. User entities are responsible for implementing a threat detection system to monitor web traffic and suspicious activity. For anomalous traffic activity identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.
25. User entities are responsible for documenting network diagrams to document system boundaries and connections to external networks with at least an annual review.
26. User entities are responsible for documenting policies and procedures for authentication that are communicated to all personnel including guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.
27. User entities are responsible for development and documentation of policy to outline requirements for access control.
28. User entities are responsible for documentation of policy to outline requirements for audit logging and monitoring of system activity at the company.
29. User entities are responsible for limiting administrative or privileged access to systems, resources, and functions to authorized personnel.
30. User entities are responsible for documentation and implementation of policy around minimum requirements for passwords used for authentication to systems.
31. User entities are responsible for configuring audit logs for system components and sensitive data in accordance with policies.
32. User entities are responsible for implementing and managing processes for the security of ePHI information.
33. User entities are responsible for sending automated notifications to personnel in the event of a backup failure. Backup failures are investigated and resolved by engineering personnel following company policies and procedures.
34. User entities are responsible for performing backup and retention of production data in accordance with the retention periods established in company policies and procedures.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to the Security Category)
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 entity to meet its objectives. 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.

HEALTH INFORMATION SECURITY PROGRAM

Glooko has developed a health information security management program to meet the information security and compliance requirements related to Managed IT services and its customer base. The program incorporates the elements of HIPAA and HITECH. The description below is a summary of safeguards that Glooko has implemented to adhere to the applicable components of HIPAA Final Security Rule and the breach notification requirements of HITECH.

Administrative Safeguards - Policies and procedures designed to show how Glooko complies with the act:

- Management has adopted a written set of health information security policies and designated the information security officer to be responsible for developing and implementing the required policies and procedures.
- Procedures address access to authorization, establishment, modification, and termination.
- Documented incident response policies for reporting security incidents are in place to guide employees in identifying, reporting, of security incidents.
- Business continuity plans are documented to enable continuation of critical business processes in the event of an emergency.
- Privileged administrative access to systems is restricted to authorized individuals.
- Automated backup systems are in place to perform scheduled replication of production data and systems at pre-defined intervals.
- Antivirus software is utilized to detect and eliminate data or files that contain certain virus signatures on certain production servers.

Physical Safeguards - Controlling physical access to protected data:

- Documented physical security policies and procedures are in place to guide personnel in physical security administration.
- Physical access procedures are in place restrict access, log visitors, and terminate access to the office facility.
- Inventory listings are utilized to track and monitor hardware and removable media.
- Data destruction procedures are in place to guide the secure disposal of data and media.

Technical Safeguards - Controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient:

- Access to in-scope systems is restricted to authorized personnel based on a valid user account and password.
- Systems are configured to enforce pre-determined thresholds to lock user sessions due to invalid login attempts.
- Security monitoring applications and manual reviews are utilized to monitor and analyze the in-scope systems for possible or actual security breaches.

Organizational Requirements - Adherence to policies and procedures in regard to PHI documentation availability, as well as documentation retention:

- Documented policies address the confidentiality threshold of PHI documents and the length of time they should be retained before being destroyed.
- Contractual responsibilities by subparts of an organization are written and maintained in contracts.
- Separation of duties is existent in order to protect confidentiality, availability, and integrity of PHI.
- Ensure that only appropriate parties gain access to PHI internally and external to the organization.

Breach Notification - A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach:

- Documented policies and procedures are in place to guide personnel in notifying the covered entity upon discovery of a breach.
- Documented policies and procedures are in place to guide personnel in responding to the discovery of a breach.

- Documented policies and procedures require disclosure of the unsecured protected health information and include, to the extent possible, the identification of each individual and a description of the event.
- Documented policies and procedures are in place to guide personnel in the exception processes of delaying and documenting notifications.
- Documented policies and procedures are in place to guide personnel in documentation of administrative requirements for demonstrating that all notifications were made as required.

Control Activities Specified by the Service Organization

The applicable trust services criteria and HIPAA/HITECH requirements, risks, and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section. Although the applicable trust services criteria and HIPAA/HITECH requirements and related control activities are included in Section 4, they are, nevertheless, an integral part of Glooko' description of the system. Any applicable trust services criteria and HIPAA/HITECH requirements that are not addressed by control activities at Glooko are described within Section 4 and within the "Subservice Organizations" and "Criteria Not Applicable to the System" sections above.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

SECTION 4

TRUST SERVICES CATEGORY, CRITERIA, HIPAA/HITECH REQUIREMENTS, RELATED CONTROLS, AND TESTS OF CONTROLS

GUIDANCE REGARDING TRUST SERVICES CATEGORY, CRITERIA, HIPAA/HITECH REQUIREMENTS, RELATED CONTROLS, AND TESTS OF CONTROLS

A-LIGN ASSURANCE's examination of the controls of Glooko was limited to the Trust Services Criteria and HIPAA/HITECH requirements, related criteria and control activities specified by the management of Glooko and did not encompass all aspects of Glooko's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the applicable trust services criteria;
- Understand the aspects of the service organization's controls that may affect the HIPAA/HITECH requirements;
- Understand the infrastructure, software, procedures and data that are designed, implemented and operated by the service organization;
- Understand the flow of ePHI through the service organization;
- Determine whether the criteria are relevant to the user entity's assertions;
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria; and
- Determine whether the service organization's controls are suitably designed to meet the health information security program of the user entity's and determine whether they have been implemented.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Personnel responsibilities for information security are communicated to and acknowledged by personnel.	Inquired of the VP, Security and IT Operations regarding onboarding process to determine that personnel responsibilities for information security, were communicated to and acknowledged by personnel.	No exceptions noted.
			Inspected the company policy acknowledgment for a sample of new hires to determine that personnel responsibilities for information security, were communicated to and acknowledged by personnel.	No exceptions noted.
		Management conducts annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	Inspected the code of conduct and completed performance and conduct evaluation form for a sample of current employees to determine that management conducted annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	No exceptions noted.
		Background checks are conducted on eligible personnel prior to hire as permitted by local laws.	Inquired of the VP, Security and IT Operations regarding background checks to determine that background checks were conducted on eligible personnel prior to hire as permitted by local laws.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the access control policies and procedures to determine that background checks were conducted on eligible personnel prior to hire as permitted by local laws.	No exceptions noted.
			Inspected the completed background check for a sample of new hires to determine that background checks were conducted on eligible personnel prior to hire as permitted by local laws.	Testing of the control activity disclosed that background check was not conducted in a timely manner for one of one new hire sampled.
		The Company maintains a documented Code of Conduct. Eligible personnel are required to accept the Company's Code of Conduct during onboarding.	Inspected the code of conduct policies and procedures and a sample of code of conduct acknowledgements for a sample of new hires and current employees to determine that the Company maintained a documented Code of Conduct, and eligible personnel were required to accept the Company's Code of Conduct during onboarding.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has a defined disciplinary sanctions process to be enacted when a member of the workforce violates the Company's policies or causes a security or privacy incident. Management retains documentation of instances when the disciplinary process was enacted.	Inquired of the VP, Security and IT Operations regarding the disciplinary process to determine that the company had a defined disciplinary process to be enacted when a member of the workforce violated the company's policies or caused a security or privacy incident, and management retained documentation of instances when the disciplinary process was enacted.	No exceptions noted.
			Inspected the code of conduct to determine that the Company had a defined disciplinary sanctions process to be enacted when a member of the workforce violated the Company's policies or caused a security or privacy incident. Management retained documentation of instances when the disciplinary process was enacted.	No exceptions noted.
			Inspected the HR records to determine that the Company had a defined disciplinary sanctions process to be enacted when a member of the workforce violated the Company's policies or caused a security or privacy incident, and management retained documentation of instances when the disciplinary process was enacted.	Testing of the control activity disclosed that there were no instances where a member of the workforce violated the company's policies or caused a security or privacy incident during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Internal communication channels are in place for employees to report failures, events, incidents, concerns, and other issues to company management.	Inspected the company's website, compliance automation software, code of conduct, internal communication channel and incident management and escalation policies and procedures to determine that internal communication channels were in place for employees to report failures, events, incidents, concerns, and other issues to company management.	No exceptions noted.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The Company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the company's charter to determine that the Company's board of directors had a documented charter that outlined its oversight responsibilities for internal control.	No exceptions noted.
		The company's board of directors meets at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies. Meeting minutes, including decisions made and action items, are documented.	Inspected the internal controls and operations review management meeting minutes to determine that the Company's board of directors met at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies, and meeting minutes, including decisions made and action items, were documented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected the compliance automation software to determine that the Company used compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.
		Management conducts annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	Inspected the code of conduct and completed performance and conduct evaluation form for a sample of current employees to determine that management conducted annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	No exceptions noted.
		The board of directors includes members independent from management who are not involved in control operations.	Inspected the company's charter and management review meeting minutes to determine that the board of directors included members independent from management who were not involved in control operations.	No exceptions noted.
		Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	Inspected the risk management policies and procedures to determine that management had defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	An organizational chart is in place to describe the organizational structure and reporting lines. The chart is available to all employees and is updated upon changes to the organizational structure.	Inspected the organizational chart, including the revision history, to determine that an organizational chart was in place to describe the organizational structure and reporting lines, and the chart was available to all employees and was updated upon changes to the organizational structure.	No exceptions noted.
		The Company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the company's charter to determine that the Company's board of directors had a documented charter that outlined its oversight responsibilities for internal control.	No exceptions noted.
		Personnel responsibilities for information security are communicated to and acknowledged by personnel.	Inquired of the VP, Security and IT Operations regarding onboarding process to determine that personnel responsibilities for information security, were communicated to and acknowledged by personnel.	No exceptions noted.
			Inspected the company policy acknowledgment for a sample of new hires to determine that personnel responsibilities for information security, were communicated to and acknowledged by personnel.	No exceptions noted.
		The board of directors includes members independent from management who are not involved in control operations.	Inspected the company's charter and management review meeting minutes to determine that the board of directors included members independent from management who were not involved in control operations.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has documented job descriptions for each position at the company, which include roles and responsibilities as well as required qualifications, skills, and experience for the role.	Inspected the job description for a sample of job roles to determine that the Company had documented job descriptions for each position at the company, which included roles and responsibilities as well as required qualifications, skills, and experience for the role.	No exceptions noted.
		The Company performs due diligence activities prior to engaging with a new service provider or vendor. Results of the due diligence activities including action items are documented.	Inspected the vendor listing and completed supplier evaluation form for a sample of third-parties to determine that the Company performed due diligence activities prior to engaging with a new service provider or vendor, and the results of the due diligence activities including action items were documented.	No exceptions noted.
		The Company obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, are documented.	Inspected the compliance reports and associated review documentation for a sample of third-parties to determine that the Company obtained and reviewed compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, were documented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The Company has established training programs to help personnel gain awareness of information security best practices. Personnel are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary.	Inspected the information security policies and procedures and training completion certificates for a sample of new hires and current employees to determine that the Company had established training programs to help personnel gain awareness of information security best practices, personnel were required to complete the training during onboarding, and periodic refresher training is provided to personnel at least annually and as deemed necessary.	No exceptions noted.
		Management conducts annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	Inspected the code of conduct and completed performance and conduct evaluation form for a sample of current employees to determine that management conducted annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	No exceptions noted.
		Background checks are conducted on eligible personnel prior to hire as permitted by local laws.	Inquired of the VP, Security and IT Operations regarding background checks to determine that background checks were conducted on eligible personnel prior to hire as permitted by local laws.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the access control policies and procedures to determine that background checks were conducted on eligible personnel prior to hire as permitted by local laws.	No exceptions noted.
			Inspected the completed background check for a sample of new hires to determine that background checks were conducted on eligible personnel prior to hire as permitted by local laws.	Testing of the control activity disclosed that background check was not conducted in a timely manner for one of one new hire sampled.
		Management evaluates candidates for employment through a formal screening process. The process may include verification of academic and professional qualifications, identity verifications, validation of personal or professional references, technical interviews, or other steps as deemed applicable by the organization.	Inspected the interview meeting schedule for a sample of new hires to determine that management evaluated candidates for employment through a formal interview process. The process included verification of academic and professional qualifications, identity verifications, validation of personal or professional references, technical interviews, or other steps as deemed applicable by the organization.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company performs due diligence activities prior to engaging with a new service provider or vendor. Results of the due diligence activities including action items are documented.	Inspected the vendor listing and completed supplier evaluation form for a sample of third-parties to determine that the Company performed due diligence activities prior to engaging with a new service provider or vendor, and the results of the due diligence activities including action items were documented.	No exceptions noted.
		The Company obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, are documented.	Inspected the compliance reports and associated review documentation for a sample of third-parties to determine that the Company obtained and reviewed compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, were documented.	No exceptions noted.
		Policies and procedures are in place that outline the talent acquisition, performance evaluation and annual training processes.	Inspected the employee performance evaluation policies and procedures and competency and training requirements policies and procedures to determine that policies and procedures were in place that outlined the talent acquisition, performance evaluation and annual training processes.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	An organizational chart is in place to describe the organizational structure and reporting lines. The chart is available to all employees and is updated upon changes to the organizational structure.	Inspected the organizational chart, including the revision history, to determine that an organizational chart was in place to describe the organizational structure and reporting lines, and the chart was available to all employees and was updated upon changes to the organizational structure.	No exceptions noted.
		Personnel responsibilities for information security are communicated to and acknowledged by personnel.	Inquired of the VP, Security and IT Operations regarding onboarding process to determine that personnel responsibilities for information security, were communicated to and acknowledged by personnel.	No exceptions noted.
			Inspected the company policy acknowledgment for a sample of new hires to determine that personnel responsibilities for information security, were communicated to and acknowledged by personnel.	No exceptions noted.
		Management conducts annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	Inspected the code of conduct and completed performance and conduct evaluation form for a sample of current employees to determine that management conducted annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company maintains a documented Code of Conduct. Eligible personnel are required to accept the Company's Code of Conduct during onboarding.	Inspected the code of conduct policies and procedures and a sample of code of conduct acknowledgements for a sample of new hires and current employees to determine that the Company maintained a documented Code of Conduct, and eligible personnel were required to accept the Company's Code of Conduct during onboarding.	No exceptions noted.
		The Company has documented job descriptions for each position at the company, which include roles and responsibilities as well as required qualifications, skills, and experience for the role.	Inspected the job description for a sample of job roles to determine that the Company had documented job descriptions for each position at the company, which included roles and responsibilities as well as required qualifications, skills, and experience for the role.	No exceptions noted.
		The Company has a defined disciplinary sanctions process to be enacted when a member of the workforce violates the Company's policies or causes a security or privacy incident. Management retains documentation of instances when the disciplinary process was enacted.	Inquired of the VP, Security and IT Operations regarding the disciplinary process to determine that the company had a defined disciplinary process to be enacted when a member of the workforce violated the company's policies or caused a security or privacy incident, and management retained documentation of instances when the disciplinary process was enacted.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the code of conduct to determine that the Company had a defined disciplinary sanctions process to be enacted when a member of the workforce violated the Company's policies or caused a security or privacy incident. Management retained documentation of instances when the disciplinary process was enacted.	No exceptions noted.
			Inspected the HR records to determine that the Company had a defined disciplinary sanctions process to be enacted when a member of the workforce violated the Company's policies or caused a security or privacy incident, and management retained documentation of instances when the disciplinary process was enacted.	Testing of the control activity disclosed that there were no instances where a member of the workforce violated the company's policies or caused a security or privacy incident during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The Company has defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	Inspected the information security policies and topic-specific policies to determine that the Company had defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	No exceptions noted.
		A documented network diagram is in place to document system boundaries and connections to external networks. The diagram is reviewed and approved by management at least annually and updated as necessary when there are changes to the environment.	Inspected the network diagram, including the version history, to determine that a documented network diagram was in place to document system boundaries and connections to external networks, and the network diagram was reviewed and approved by management at least annually and updated as necessary when there were changes to the environment.	No exceptions noted.
		Company policies are accessible to all employees and, as applicable, third-parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	Inspected the compliance automation software and information security policy acknowledgements for a sample of new hires and current employees to determine that Company policies were accessible to all employees and, as applicable, third-parties such as contractors, and personnel were required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary.	Inspected the information security policies version history and records of approvals to determine that management reviewed and approved company policies at least annually, and updates to the policies were made as deemed necessary.	No exceptions noted.
		Network security controls are in place to restrict public access to remote server administration ports to authorized IP addresses or address ranges only.	Inspected the security groups and associated inbound and outbound rules to determine that network security controls were in place to restrict public access to remote server administration ports to authorized IP addresses or address ranges only.	No exceptions noted.
		Cloud resources are configured to deny public access.	Inspected the security groups and associated inbound and outbound rules to determine that cloud resources were configured to deny public access.	No exceptions noted.
		Network security configurations are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.	Inspected the network diagram and security groups and associated inbound and outbound rules to determine that network security configurations were in place to limit inbound and outbound traffic to the environment to only what was necessary based on business justification, and all other traffic was specifically denied.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		An IDS is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected.	Inspected the network diagram and IDS configurations to determine that an IDS was in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and was configured to alert personnel when a potential intrusion was detected.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The Company has defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	Inspected the information security policies and topic-specific policies to determine that the Company had defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The company's board of directors meets at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies. Meeting minutes, including decisions made and action items, are documented.	Inspected the internal controls and operations review management meeting minutes to determine that the Company's board of directors met at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies, and meeting minutes, including decisions made and action items, were documented.	No exceptions noted.
		Personnel responsibilities for information security are communicated to and acknowledged by personnel.	Inquired of the VP, Security and IT Operations regarding onboarding process to determine that personnel responsibilities for information security, were communicated to and acknowledged by personnel.	No exceptions noted.
			Inspected the company policy acknowledgment for a sample of new hires to determine that personnel responsibilities for information security, were communicated to and acknowledged by personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Company policies are accessible to all employees and, as applicable, third-parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	Inspected the compliance automation software and information security policy acknowledgements for a sample of new hires and current employees to determine that Company policies were accessible to all employees and, as applicable, third-parties such as contractors, and personnel were required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	No exceptions noted.
		Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary.	Inspected the information security policies version history and records of approvals to determine that management reviewed and approved company policies at least annually, and updates to the policies were made as deemed necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has established training programs to help personnel gain awareness of information security best practices. Personnel are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary.	Inspected the information security policies and procedures and training completion certificates for a sample of new hires and current employees to determine that the Company had established training programs to help personnel gain awareness of information security best practices, personnel were required to complete the training during onboarding, and periodic refresher training is provided to personnel at least annually and as deemed necessary.	No exceptions noted.
		Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	Inspected the risk management policies and procedures to determine that management had defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	No exceptions noted.
		The Company maintains a documented Code of Conduct. Eligible personnel are required to accept the Company's Code of Conduct during onboarding.	Inspected the code of conduct policies and procedures and a sample of code of conduct acknowledgements for a sample of new hires and current employees to determine that the Company maintained a documented Code of Conduct, and eligible personnel were required to accept the Company's Code of Conduct during onboarding.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has documented job descriptions for each position at the company, which include roles and responsibilities as well as required qualifications, skills, and experience for the role.	Inspected the job description for a sample of job roles to determine that the Company had documented job descriptions for each position at the company, which included roles and responsibilities as well as required qualifications, skills, and experience for the role.	No exceptions noted.
		The Company provides external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer communications are responded to within defined SLAs.	Inquired of the VP, Security and IT Operations regarding customer support issues to determine that the company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.
			Inspected the incident management and escalation policies and procedures to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting ticket for a sample of customer support issues to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	Testing of the control activity disclosed that there were no customer support issues during the review period.
		Internal communication channels are in place for employees to report failures, events, incidents, concerns, and other issues to company management.	Inspected the company's website, compliance automation software, code of conduct, internal communication channel and incident management and escalation policies and procedures to determine that internal communication channels were in place for employees to report failures, events, incidents, concerns, and other issues to company management.	No exceptions noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company's board of directors meets at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies. Meeting minutes, including decisions made and action items, are documented.	Inspected the internal controls and operations review management meeting minutes to determine that the Company's board of directors met at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies, and meeting minutes, including decisions made and action items, were documented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Personnel responsibilities for information security are communicated to and acknowledged by personnel.	Inquired of the VP, Security and IT Operations regarding onboarding process to determine that personnel responsibilities for information security, were communicated to and acknowledged by personnel.	No exceptions noted.
			Inspected the company policy acknowledgment for a sample of new hires to determine that personnel responsibilities for information security, were communicated to and acknowledged by personnel.	No exceptions noted.
		The Company maintains a third-party register that includes a complete and accurate list of third-parties, relationship owners, description for each of the services provided, risk ratings, results of third-party risk management activities, etc. The Company executes agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outline the responsibilities of each vendor or service provider.	Inspected the third-party register to determine that the Company maintained a third-party register that included a complete and accurate list of third-parties, relationship owners, description for each of the services provided, risk ratings, results of third-party risk management activities, etc., and the Company executed agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outlined the responsibilities of each vendor or service provider.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the third-party agreement for a sample of third-parties to determine that the Company maintained a third-party register that included a complete and accurate list of third-parties, relationship owners, description for each of the services provided, risk ratings, results of third-party risk management activities, etc., and the Company executed agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outlined the responsibilities of each vendor or service provider.	No exceptions noted.
		The company maintains a publicly available ToS for use of the system. All users must agree to the ToS prior to using the system.	Inspected the company's website and the publicly available ToS to determine that the company maintained a publicly available ToS for use of the system, and users had to agree to the ToS prior to using the system.	No exceptions noted.
		The Company communicates service commitments and system requirements to customers through contracts, agreements, company website, etc. The Company provides notification to relevant parties of any changes to service commitments and system requirements.	Inspected the customer agreement for a sample of customers to determine that the Company communicated service commitments and system requirements to customers through contracts, agreements, company website, etc., and the Company provided notification to relevant parties of any changes to services commitments and system requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company provides user guides, help articles, system documentation or other mechanisms to users to share information about the design and operation of the system and its boundaries. The information provided includes functional and nonfunctional requirements related to system processing and information specifications required to support the use of the system.	Inspected the company's website and user guides to determine that the Company provided user guides, help articles, system documentation or other mechanisms to users to share information about the design and operation of the system and its boundaries, and the information provided included functional and nonfunctional requirements related to system processing and information specifications required to support the use of the system.	No exceptions noted.
		The Company provides external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer communications are responded to within defined SLAs.	Inquired of the VP, Security and IT Operations regarding customer support issues to determine that the company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.
			Inspected the incident management and escalation policies and procedures to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting ticket for a sample of customer support issues to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	Testing of the control activity disclosed that there were no customer support issues during the review period.
		Internal communication channels are in place for employees to report failures, events, incidents, concerns, and other issues to company management.	Inspected the company's website, compliance automation software, code of conduct, internal communication channel and incident management and escalation policies and procedures to determine that internal communication channels were in place for employees to report failures, events, incidents, concerns, and other issues to company management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The Company has defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	Inspected the information security policies and topic-specific policies to determine that the Company had defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	No exceptions noted.
		An organizational chart is in place to describe the organizational structure and reporting lines. The chart is available to all employees and is updated upon changes to the organizational structure.	Inspected the organizational chart, including the revision history, to determine that an organizational chart was in place to describe the organizational structure and reporting lines, and the chart was available to all employees and was updated upon changes to the organizational structure.	No exceptions noted.
		The Company has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	Inspected the risk assessment policies and procedures to determine that the Company had defined and documented a process for risk assessment and risk management that outlined the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented.	Inspected the completed risk assessment to determine that the Company conducted risks assessments annually as required by company policy and compliance requirements, the risk assessment included consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk, a risk owner was assigned to each risk, every risk was assigned a risk treatment option, and the results of the risk assessment were documented.	No exceptions noted.
		The Company uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected the compliance automation software to determine that the Company used compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.
		Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected the completed risk assessment to determine that management had documented a risk treatment plan to formally manage risks identified in risk assessment activities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Company policies are accessible to all employees and, as applicable, third-parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	Inspected the compliance automation software and information security policy acknowledgements for a sample of new hires and current employees to determine that Company policies were accessible to all employees and, as applicable, third-parties such as contractors, and personnel were required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	No exceptions noted.
		Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary.	Inspected the information security policies version history and records of approvals to determine that management reviewed and approved company policies at least annually, and updates to the policies were made as deemed necessary.	No exceptions noted.
		Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	Inspected the risk management policies and procedures to determine that management had defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company communicates service commitments and system requirements to customers through contracts, agreements, company website, etc. The Company provides notification to relevant parties of any changes to service commitments and system requirements.	Inspected the customer agreement for a sample of customers to determine that the Company communicated service commitments and system requirements to customers through contracts, agreements, company website, etc., and the Company provided notification to relevant parties of any changes to services commitments and system requirements.	No exceptions noted.
		Management has defined company objectives, including mission and vision statements, operational objectives at the entity and functional levels, financial performance goals, and other objectives as appropriate, to serve as the basis for risk assessment activities. Management communicates its objectives and any changes to those objectives to personnel.	Inspected the annual management internal controls review meeting minutes and compliance automation software to determine that management had defined company objectives, including mission and vision statements, operational objectives at the entity and functional levels, financial performance goals, and other objectives as appropriate, to serve as the basis for risk assessment activities and management communicated its objectives and any changes to those objectives to personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.2	COSO Principle 7: 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.	The Company has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	Inspected the risk assessment policies and procedures to determine that the Company had defined and documented a process for risk assessment and risk management that outlined the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	No exceptions noted.
		The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented.	Inspected the completed risk assessment to determine that the Company conducted risks assessments annually as required by company policy and compliance requirements, the risk assessment included consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk, a risk owner was assigned to each risk, every risk was assigned a risk treatment option, and the results of the risk assessment were documented.	No exceptions noted.
		Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected the completed risk assessment to determine that management had documented a risk treatment plan to formally manage risks identified in risk assessment activities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company performs due diligence activities prior to engaging with a new service provider or vendor. Results of the due diligence activities including action items are documented.	Inspected the vendor listing and completed supplier evaluation form for a sample of third-parties to determine that the Company performed due diligence activities prior to engaging with a new service provider or vendor, and the results of the due diligence activities including action items were documented.	No exceptions noted.
		The Company obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, are documented.	Inspected the compliance reports and associated review documentation for a sample of third-parties to determine that the Company obtained and reviewed compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, were documented.	No exceptions noted.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The Company has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	Inspected the risk assessment policies and procedures to determine that the Company had defined and documented a process for risk assessment and risk management that outlined the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented.	Inspected the completed risk assessment to determine that the Company conducted risks assessments annually as required by company policy and compliance requirements, the risk assessment included consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk, a risk owner was assigned to each risk, every risk was assigned a risk treatment option, and the results of the risk assessment were documented.	No exceptions noted.
		Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected the completed risk assessment to determine that management had documented a risk treatment plan to formally manage risks identified in risk assessment activities.	No exceptions noted.
		The Company performs an evaluation of fraud risks at least annually, either as a separate evaluation or as part of the overall enterprise risk assessment. The evaluation of fraud risk is performed in accordance with the company's risk assessment methodology.	Inspected the completed risk assessment to determine that the Company performed an evaluation of fraud risks at least annually, either as a separate evaluation or as part of the overall enterprise risk assessment, and the evaluation of fraud risk was performed in accordance with the company's risk assessment methodology.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The Company has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	Inspected the risk assessment policies and procedures to determine that the Company had defined and documented a process for risk assessment and risk management that outlined the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	No exceptions noted.
		The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented.	Inspected the completed risk assessment to determine that the Company conducted risks assessments annually as required by company policy and compliance requirements, the risk assessment included consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk, a risk owner was assigned to each risk, every risk was assigned a risk treatment option, and the results of the risk assessment were documented.	No exceptions noted.
		The Company uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected the compliance automation software to determine that the Company used compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected the completed risk assessment to determine that management had documented a risk treatment plan to formally manage risks identified in risk assessment activities.	No exceptions noted.
		The Company performs due diligence activities prior to engaging with a new service provider or vendor. Results of the due diligence activities including action items are documented.	Inspected the vendor listing and completed supplier evaluation form for a sample of third-parties to determine that the Company performed due diligence activities prior to engaging with a new service provider or vendor, and the results of the due diligence activities including action items were documented.	No exceptions noted.
		The Company obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, are documented.	Inspected the compliance reports and associated review documentation for a sample of third-parties to determine that the Company obtained and reviewed compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, were documented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Changes to the entity's systems, applications, technologies, tools, and leadership are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that changes to the entity's systems, applications, technologies, tools, and leadership were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Management performs user access reviews to validate user accounts, including third-party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical access as necessary. Changes resulting from the review, if any, are documented and implemented.	Inspected the completed network user access review to determine that management performed user access reviews to validate user accounts, including third-party or vendor accounts, and their associated privileges remained appropriate, the review included validation of logical access as necessary, and changes resulting from the review, if any, were documented and implemented.	No exceptions noted.
		The Company has defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	Inspected the information security policies and topic-specific policies to determine that the Company had defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	No exceptions noted.
		The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented.	Inspected the completed risk assessment to determine that the Company conducted risks assessments annually as required by company policy and compliance requirements, the risk assessment included consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk, a risk owner was assigned to each risk, every risk was assigned a risk treatment option, and the results of the risk assessment were documented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected the compliance automation software to determine that the Company used compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.
		Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected the completed risk assessment to determine that management had documented a risk treatment plan to formally manage risks identified in risk assessment activities.	No exceptions noted.
		The company has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloguing, and assigning risk ratings to vulnerabilities to prioritize remediation efforts.	Inspected the vulnerability management policies and procedures to determine that the company had a defined policy that established requirements for vulnerability management across the organization, including monitoring, cataloguing, and assigning risk ratings to vulnerabilities to prioritize remediation efforts.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		An external penetration test of production environments is performed by an independent third-party annually. Results are reviewed by management and vulnerabilities are tracked to resolution in accordance with company policies.	Inspected the completed penetration test results and associated resolution documentation to determine that an external penetration test of production environments was performed by an independent third-party annually and the results were reviewed by management and vulnerabilities were tracked to resolution in accordance with company policies.	No exceptions noted.
		Company policies are accessible to all employees and, as applicable, third-parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	Inspected the compliance automation software and information security policy acknowledgements for a sample of new hires and current employees to determine that Company policies were accessible to all employees and, as applicable, third-parties such as contractors, and personnel were required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	No exceptions noted.
		Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary.	Inspected the information security policies version history and records of approvals to determine that management reviewed and approved company policies at least annually, and updates to the policies were made as deemed necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management conducts annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	Inspected the code of conduct and completed performance and conduct evaluation form for a sample of current employees to determine that management conducted annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	No exceptions noted.
		Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	Inspected the risk management policies and procedures to determine that management had defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	No exceptions noted.
		The Company performs due diligence activities prior to engaging with a new service provider or vendor. Results of the due diligence activities including action items are documented.	Inspected the vendor listing and completed supplier evaluation form for a sample of third-parties to determine that the Company performed due diligence activities prior to engaging with a new service provider or vendor, and the results of the due diligence activities including action items were documented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, are documented.	Inspected the compliance reports and associated review documentation for a sample of third-parties to determine that the Company obtained and reviewed compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, were documented.	No exceptions noted.
		Production systems and resources are monitored and automated alerts are sent out personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalated per policy if necessary.	Inspected the monitoring tool configurations, the anti-malware software dashboard console, source code repository configurations, IDS configurations, firewall rule sets for a sample of production servers, and the anti-malware, source code repository, and IDS alert configurations and an example alert to determine that production systems and resources were monitored and automated alerts were sent out personnel based on pre-configured rules, and events were triaged to determine if they constituted an incident and escalated per policy if necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC4.2	COSO Principle 17: 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.	The company's board of directors meets at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies. Meeting minutes, including decisions made and action items, are documented.	Inspected the internal controls and operations review management meeting minutes to determine that the Company's board of directors met at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies, and meeting minutes, including decisions made and action items, were documented.	No exceptions noted.
		The Company uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected the compliance automation software to determine that the Company used compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.
		Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected the completed risk assessment to determine that management had documented a risk treatment plan to formally manage risks identified in risk assessment activities.	No exceptions noted.
		Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	Inspected the risk management policies and procedures to determine that management had defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The Company uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected the compliance automation software to determine that the Company used compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.
		The Company has a defined business continuity plan that outlines strategies for maintaining operations during a disruption.	Inspected the business continuity plan to determine that the Company had a defined business continuity plan that outlined strategies for maintaining operations during a disruption.	No exceptions noted.
		Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected the completed risk assessment to determine that management had documented a risk treatment plan to formally manage risks identified in risk assessment activities.	No exceptions noted.
		The Company has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	Inspected the disaster recovery plans to determine that the Company had a documented disaster recovery plan that outlined roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	No exceptions noted.
		The Company conducts tests of the disaster recovery plans at least annually. Results and lessons learned are documented, and updates to the plans are made as necessary.	Inspected the completed disaster recovery test results to determine that the Company conducted tests of the disaster recovery plans at least annually, and the results and lessons learned were documented, and updates to the plans were made as necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The board of directors includes members independent from management who are not involved in control operations.	Inspected the company's charter and management review meeting minutes to determine that the board of directors included members independent from management who were not involved in control operations.	No exceptions noted.
		Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	Inspected the risk management policies and procedures to determine that management had defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The Company has defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	Inspected the information security policies and topic-specific policies to determine that the Company had defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	No exceptions noted.
		The Company uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected the compliance automation software to determine that the Company used compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Company policies are accessible to all employees and, as applicable, third-parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	Inspected the compliance automation software and information security policy acknowledgements for a sample of new hires and current employees to determine that Company policies were accessible to all employees and, as applicable, third-parties such as contractors, and personnel were required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	No exceptions noted.
		Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary.	Inspected the information security policies version history and records of approvals to determine that management reviewed and approved company policies at least annually, and updates to the policies were made as deemed necessary.	No exceptions noted.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The Company has defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	Inspected the information security policies and topic-specific policies to determine that the Company had defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected the compliance automation software to determine that the Company used compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.
		Company policies are accessible to all employees and, as applicable, third-parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	Inspected the compliance automation software and information security policy acknowledgements for a sample of new hires and current employees to determine that Company policies were accessible to all employees and, as applicable, third-parties such as contractors, and personnel were required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	No exceptions noted.
		Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary.	Inspected the information security policies version history and records of approvals to determine that management reviewed and approved company policies at least annually, and updates to the policies were made as deemed necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	Inspected the risk management policies and procedures to determine that management had defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	No exceptions noted.
		The Company has documented job descriptions for each position at the company, which include roles and responsibilities as well as required qualifications, skills, and experience for the role.	Inspected the job description for a sample of job roles to determine that the Company had documented job descriptions for each position at the company, which included roles and responsibilities as well as required qualifications, skills, and experience for the role.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**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.	The Company has developed and documented a policy that outlines requirements for access control.	Inspected the system access control policies and procedures to determine that the Company had developed and documented a policy that outlined requirements for access control.	No exceptions noted.
		Management performs user access reviews to validate user accounts, including third-party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical access as necessary. Changes resulting from the review, if any, are documented and implemented.	Inspected the completed network user access review to determine that management performed user access reviews to validate user accounts, including third-party or vendor accounts, and their associated privileges remained appropriate, the review included validation of logical access as necessary, and changes resulting from the review, if any, were documented and implemented.	No exceptions noted.
		A centralized asset register is maintained for physical, cloud, and other assets that includes descriptive attributes for asset accountability such as owner, description, location, classification, and other information based on the type of asset. Processes are in place to maintain an updated inventory through manual reviews or automated mechanisms.	Inspected the inventory listing of system assets and components, including the revision history, and compliance automation software to determine that a centralized asset register was maintained for physical, cloud, and other assets that included descriptive attributes for asset accountability such as owner, description, location, classification, and other information based on the type of asset, and processes were in place to maintain an updated inventory through manual reviews or automated mechanisms.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Key-management policies and procedures are documented and implemented including: generation of strong cryptographic keys, secure distribution, and secure storage of cryptographic keys used to protect sensitive data.	Inspected the encryption policies and procedures to determine that key-management policies and procedures were documented and implemented including: generation of strong cryptographic keys, secure distribution, and secure storage of cryptographic keys used to protect sensitive data.	No exceptions noted.
		The Company retires, replaces or destructs cryptographic keys that are no longer used or needed or when the key expires, the integrity of the key has been weakened, or the key is known or suspected to be compromised, in accordance with documented company policies and procedures. Retired or replaced keys are not used for encryption operations.	Inspected the encryption policies and procedures to determine that the Company retired, replaced or destructed cryptographic keys that were no longer used or needed or when the key expired, the integrity of the key was weakened, or the key was known or suspected to be compromised, in accordance with documented company policies and procedures, and retired or replaced keys were not used for encryption operations.	No exceptions noted.
		Invalid authentication attempts are limited by locking out the user ID after not more than five failed attempts.	Inspected the network account lockout settings to determine that invalid authentication attempts were limited by locking out the user ID after not more than five failed attempts.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has configured account lockout duration following a set number of invalid authentication attempts to a minimum of 60 minutes or until the identity of the user is confirmed.	Inspected the network account lockout duration settings to determine that the Company had configured account lockout duration following a set number of invalid authentication attempts to a minimum of 60 minutes or until the identity of the user was confirmed.	No exceptions noted.
		The Company has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	Inspected the system access control policies and procedures, password policies and procedures and compliance automation software to determine that the Company had documented policies and procedures for authentication that were communicated to all personnel, and that these documents included guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Audit logs are enabled and active for system components and sensitive data in accordance with company policies.	Inspected the information security and logging and monitoring policies and procedures and network audit logging settings and an example audit log extract to determine that audit logs were enabled and active for system components and sensitive data in accordance with company policies.	No exceptions noted.
		Data at rest is encrypted using strong cryptographic algorithms.	Inspected the encryption configurations for data at rest to determine that data at rest was encrypted using strong cryptographic algorithms.	No exceptions noted.
		Data in transit is encrypted using strong cryptographic algorithms.	Inspected the encryption configurations for data in transit to determine that data in transit was encrypted using strong cryptographic algorithms.	No exceptions noted.
		Group, shared, or generic account usage is prevented unless strictly necessary and supported by documented business justification and management approval. Mechanisms are in place to confirm individual user identity before access to the account is granted and to trace every action to an individual user.	Inquired of the VP, Security and IT Operations, regarding group, shared, or generic account usage to determine that group, shared, or generic account usage was prevented unless strictly necessary and supported by documented business justification and management approval, and mechanisms were in place to confirm individual user identity before access to the account was granted and to trace every action to an individual user.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the system access control policies and procedures to determine that group, shared, or generic account usage was prevented unless strictly necessary and supported by documented business justification and management approval, and mechanisms were in place to confirm individual user identity before access to the account was granted and to trace every action to an individual user.	No exceptions noted.
			Inspected the network user listings, documented business justifications and management approval, and authentication settings to determine that group, shared, or generic account usage was prevented unless strictly necessary and supported by documented business justification and management approval, and mechanisms were in place to confirm individual user identity before access to the account was granted and to trace every action to an individual user.	Testing of the control activity disclosed that there were no group, shared, or generic accounts used during the review period.
		Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel.	Inquired of the VP, Security and IT Operations regarding privileged access to determine that administrative or privileged access to systems, resources, and functions was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the network administrator listings and access rights to determine that administrative or privileged access to systems, resources, and functions was restricted to authorized personnel.	No exceptions noted.
		The Company has implemented technical measures to protect stored user passwords for the system.	Inspected the encryption configurations for stored user passwords to determine that the Company had implemented technical measures to protect stored user passwords for the system.	No exceptions noted.
		The Company has implemented segregation controls so that customers cannot impact or access data or resources of other customers.	Inspected the network diagram to determine that the Company had implemented segregation controls so that customers could not impact or access data or resources of other customers.	No exceptions noted.
		The Company has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy.	Inspected the system access control policies and procedures, password policies and procedures, and authentication and password configurations for the network layer and the systems storing or maintaining ePHI to determine that the Company had a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems, and password requirements were enforced for all systems in accordance with company policy.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Access requests to information resources, including access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	Inspected the system access control policies and procedures, network, application, database, operating system user listings, and user access request ticket for a sample of new hires to determine that access requests to information resources, including access to systems and data, were documented and approved by management based on least privilege, need to know, and segregation of duties principles.	No exceptions noted.
		System access is revoked within one business day of effective termination date for terminated users.	Inspected the system access control policies and procedures, internal network access user listings, and user access revocation ticket for a sample of terminated employees to determine that system and physical access was revoked within one business day of effective termination date for terminated users.	No exceptions noted.
		Authentication to systems requires the use of unique identities.	Inspected the network user listings and access rights to determine that authentication to systems required the use of unique identities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Root password authentication to production resources is disabled and only allowed for under exceptional circumstances for a limited time duration based on documented business justification and approval from management.	Inspected the system access control policies and procedures and root password authentication settings for the productions resources to determine that root password authentication to production resources was disabled and only allowed for under exceptional circumstances for a limited time duration based on documented business justification and approval from management.	No exceptions noted.
		The Company has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company.	Inspected the information security policies and procedures and logging and monitoring policies and procedures to determine that the Company had a documented policy that outlined requirements for audit logging and monitoring of system activity at the company.	No exceptions noted.
		The Company uses network segmentation to isolate portions of the environment and to control traffic between them based on security and business needs.	Inspected the network diagram to determine that the Company used network segmentation to isolate portions of the environment and to control traffic between them based on security and business needs.	No exceptions noted.
		Access to the root account in the cloud infrastructure provider is monitored. Login activity for the root account is investigated and validated for appropriateness.	Inspected the compliance automation software and supporting login documentation to determine that access to the root account in the cloud infrastructure provider was monitored, and login activity for the root account was investigated and validated for appropriateness.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	The Company has developed and documented a policy that outlines requirements for access control.	Inspected the system access control policies and procedures to determine that the Company had developed and documented a policy that outlined requirements for access control.	No exceptions noted.
		Management performs user access reviews to validate user accounts, including third-party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical access as necessary. Changes resulting from the review, if any, are documented and implemented.	Inspected the completed network user access review to determine that management performed user access reviews to validate user accounts, including third-party or vendor accounts, and their associated privileges remained appropriate, the review included validation of logical access as necessary, and changes resulting from the review, if any, were documented and implemented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	Inspected the system access control policies and procedures, password policies and procedures and compliance automation software to determine that the Company had documented policies and procedures for authentication that were communicated to all personnel, and that these documents included guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	No exceptions noted.
		Access requests to information resources, including access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	Inspected the system access control policies and procedures, network, application, database, operating system user listings, and user access request ticket for a sample of new hires to determine that access requests to information resources, including access to systems and data, were documented and approved by management based on least privilege, need to know, and segregation of duties principles.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		System access is revoked within one business day of effective termination date for terminated users.	Inspected the system access control policies and procedures, internal network access user listings, and user access revocation ticket for a sample of terminated employees to determine that system and physical access was revoked within one business day of effective termination date for terminated users.	No exceptions noted.
		The Company has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company.	Inspected the information security policies and procedures and logging and monitoring policies and procedures to determine that the Company had a documented policy that outlined requirements for audit logging and monitoring of system activity at the company.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
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.	The Company has developed and documented a policy that outlines requirements for access control.	Inspected the system access control policies and procedures to determine that the Company had developed and documented a policy that outlined requirements for access control.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management performs user access reviews to validate user accounts, including third-party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical access as necessary. Changes resulting from the review, if any, are documented and implemented.	Inspected the completed network user access review to determine that management performed user access reviews to validate user accounts, including third-party or vendor accounts, and their associated privileges remained appropriate, the review included validation of logical access as necessary, and changes resulting from the review, if any, were documented and implemented.	No exceptions noted.
		The Company has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	Inspected the system access control policies and procedures, password policies and procedures and compliance automation software to determine that the Company had documented policies and procedures for authentication that were communicated to all personnel, and that these documents included guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Access requests to information resources, including access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	Inspected the system access control policies and procedures, network, application, database, operating system user listings, and user access request ticket for a sample of new hires to determine that access requests to information resources, including access to systems and data, were documented and approved by management based on least privilege, need to know, and segregation of duties principles.	No exceptions noted.
		System access is revoked within one business day of effective termination date for terminated users.	Inspected the system access control policies and procedures, internal network access user listings, and user access revocation ticket for a sample of terminated employees to determine that system and physical access was revoked within one business day of effective termination date for terminated users.	No exceptions noted.
		The Company has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company.	Inspected the information security policies and procedures and logging and monitoring policies and procedures to determine that the Company had a documented policy that outlined requirements for audit logging and monitoring of system activity at the company.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Part of this criterion is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criterion is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
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.	The company disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.	Inquired of the VP, Security and IT Operations regarding data disposal to determine that the company disposed of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.	No exceptions noted.
			Inspected the data retention policies and procedures to determine that the company disposed of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the destruction certificate for a sample of requests to dispose of data on hardware to determine that the Company disposed of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.	Testing of the control activity disclosed that no requests to dispose of data occurred during the review period.
		The Company has documented policies and procedures for erasure or destruction of information that has been identified for disposal.	Inspected the data retention policies and procedures to determine that the company had documented and implemented policies and procedures for erasure or destruction of information that has been identified for disposal.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The deployed anti-malware solution is kept current via automatic updates and configured to detect all known types of malware and to remove, block, or contain all known types of malware.	Inspected the anti-malware settings to determine that the deployed anti-malware solution was kept current via automatic updates and configured to detect all known types of malware and to remove, block, or contain all known types of malware.	No exceptions noted.
		The implemented anti-malware solutions are configured to perform real-time scans.	Inspected the anti-malware settings to determine that the implemented anti-malware solutions were configured to perform real-time scans.	No exceptions noted.
		Anti-malware software is installed on company-managed devices.	Inspected the anti-malware software dashboard console to determine that anti-malware software was installed on company-managed devices.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the anti-malware settings for a sample of devices to determine that anti-malware software was installed on company-managed devices.	No exceptions noted.
		Data at rest is encrypted using strong cryptographic algorithms.	Inspected the encryption configurations for data at rest to determine that data at rest was encrypted using strong cryptographic algorithms.	No exceptions noted.
		Data in transit is encrypted using strong cryptographic algorithms.	Inspected the encryption configurations for data in transit to determine that data in transit was encrypted using strong cryptographic algorithms.	No exceptions noted.
		Network security controls are in place to restrict public access to remote server administration ports to authorized IP addresses or address ranges only.	Inspected the security groups and associated inbound and outbound rules to determine that network security controls were in place to restrict public access to remote server administration ports to authorized IP addresses or address ranges only.	No exceptions noted.
		Cloud resources are configured to deny public access.	Inspected the security groups and associated inbound and outbound rules to determine that cloud resources were configured to deny public access.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network security configurations are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.	Inspected the network diagram and security groups and associated inbound and outbound rules to determine that network security configurations were in place to limit inbound and outbound traffic to the environment to only what was necessary based on business justification, and all other traffic was specifically denied.	No exceptions noted.
		A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	Inspected the threat detection system and an example alert to determine that a threat detection system was in place to monitor web traffic and suspicious activity, and when anomalous traffic activity was identified, alerts were automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	No exceptions noted.
		A firewall is in place to protect public-facing web applications from outside threats.	Inspected the network diagram and the firewall configurations for the production environment to determine that a firewall was in place to protect public-facing web applications from outside threats.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		An IDS is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected.	Inspected the network diagram and IDS configurations to determine that an IDS was in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and was configured to alert personnel when a potential intrusion was detected.	No exceptions noted.
		Remote access to production systems is only available through an encrypted connection.	Inspected the encryption configurations to determine that remote access to production systems was only available through an encrypted connection.	No exceptions noted.
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.	Data at rest is encrypted using strong cryptographic algorithms.	Inspected the encryption configurations for data at rest to determine that data at rest was encrypted using strong cryptographic algorithms.	No exceptions noted.
		Data in transit is encrypted using strong cryptographic algorithms.	Inspected the encryption configurations for data in transit to determine that data in transit was encrypted using strong cryptographic algorithms.	No exceptions noted.
		Network security controls are in place to restrict public access to remote server administration ports to authorized IP addresses or address ranges only.	Inspected the security groups and associated inbound and outbound rules to determine that network security controls were in place to restrict public access to remote server administration ports to authorized IP addresses or address ranges only.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Cloud resources are configured to deny public access.	Inspected the security groups and associated inbound and outbound rules to determine that cloud resources were configured to deny public access.	No exceptions noted.
		Network security configurations are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.	Inspected the network diagram and security groups and associated inbound and outbound rules to determine that network security configurations were in place to limit inbound and outbound traffic to the environment to only what was necessary based on business justification, and all other traffic was specifically denied.	No exceptions noted.
		A firewall is in place to protect public-facing web applications from outside threats.	Inspected the network diagram and the firewall configurations for the production environment to determine that a firewall was in place to protect public-facing web applications from outside threats.	No exceptions noted.
		An IDS is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected.	Inspected the network diagram and IDS configurations to determine that an IDS was in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and was configured to alert personnel when a potential intrusion was detected.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Remote access to production systems is only available through an encrypted connection.	Inspected the encryption configurations to determine that remote access to production systems was only available through an encrypted connection.	No 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.	The deployed anti-malware solution is kept current via automatic updates and configured to detect all known types of malware and to remove, block, or contain all known types of malware.	Inspected the anti-malware settings to determine that the deployed anti-malware solution was kept current via automatic updates and configured to detect all known types of malware and to remove, block, or contain all known types of malware.	No exceptions noted.
		The implemented anti-malware solutions are configured to perform real-time scans.	Inspected the anti-malware settings to determine that the implemented anti-malware solutions were configured to perform real-time scans.	No exceptions noted.
		The Company has source code repository to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts.	Inspected the source code repository configurations to determine that the Company had source code repository to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data could not be changed without generating alerts.	No exceptions noted.
		Anti-malware software is installed on company-managed devices.	Inspected the anti-malware software dashboard console to determine that anti-malware software was installed on company-managed devices.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the anti-malware settings for a sample of devices to determine that anti-malware software was installed on company-managed devices.	No exceptions noted.
		Access to make changes in production environments is restricted to authorized personnel in accordance with segregation of duties principles and the company's documented policies and procedures.	Inquired of the VP, Security and IT Operations regarding the ability to migrate changes into the production environment to determine that access to make changes in production environments was restricted to authorized personnel in accordance with segregation of duties principles and the company's documented policies and procedures.	No exceptions noted.
			Inspected the change management policies and procedures and list of users with the ability to deploy changes into the environment to determine that access to make changes in internal environments was restricted to authorized personnel in accordance with segregation of duties principles and the company's documented policies and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production systems and resources are monitored and automated alerts are sent out personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalated per policy if necessary.	Inspected the monitoring tool configurations, the anti-malware software dashboard console, source code repository configurations, IDS configurations, firewall rule sets for a sample of production servers, and the anti-malware, source code repository, and IDS alert configurations and an example alert to determine that production systems and resources were monitored and automated alerts were sent out personnel based on pre-configured rules, and events were triaged to determine if they constituted an incident and escalated per policy if necessary.	No exceptions noted.
		A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	Inspected the threat detection system and an example alert to determine that a threat detection system was in place to monitor web traffic and suspicious activity, and when anomalous traffic activity was identified, alerts were automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**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.	The Company has identified and documented baseline security configuration standards for system components in accordance with industry-accepted hardening standards or vendor recommendations. These standards are reviewed at least annually and updated as needed.	Inspected the asset management policies and procedures and documented baseline security configuration standards, including the revision history, to determine that the Company had identified and documented baseline security configuration standards for system components in accordance with industry-accepted hardening standards or vendor recommendations, and these standards were reviewed at least annually and updated as needed and verified to be in place before or immediately after a production system component was installed or modified.	No exceptions noted.
		The company has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloguing, and assigning risk ratings to vulnerabilities to prioritize remediation efforts.	Inspected the vulnerability management policies and procedures to determine that the company had a defined policy that established requirements for vulnerability management across the organization, including monitoring, cataloguing, and assigning risk ratings to vulnerabilities to prioritize remediation efforts.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		An external penetration test of production environments is performed by an independent third-party annually. Results are reviewed by management and vulnerabilities are tracked to resolution in accordance with company policies.	Inspected the completed penetration test results and associated resolution documentation to determine that an external penetration test of production environments was performed by an independent third-party annually and the results were reviewed by management and vulnerabilities were tracked to resolution in accordance with company policies.	No exceptions noted.
		The Company has source code repository to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts.	Inspected the source code repository configurations to determine that the Company had source code repository to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data could not be changed without generating alerts.	No exceptions noted.
		Network security controls are in place to restrict public access to remote server administration ports to authorized IP addresses or address ranges only.	Inspected the security groups and associated inbound and outbound rules to determine that network security controls were in place to restrict public access to remote server administration ports to authorized IP addresses or address ranges only.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company.	Inspected the information security policies and procedures and logging and monitoring policies and procedures to determine that the Company had a documented policy that outlined requirements for audit logging and monitoring of system activity at the company.	No exceptions noted.
		Cloud resources are configured to deny public access.	Inspected the security groups and associated inbound and outbound rules to determine that cloud resources were configured to deny public access.	No exceptions noted.
		Management has defined company objectives, including mission and vision statements, operational objectives at the entity and functional levels, financial performance goals, and other objectives as appropriate, to serve as the basis for risk assessment activities. Management communicates its objectives and any changes to those objectives to personnel.	Inspected the annual management internal controls review meeting minutes and compliance automation software to determine that management had defined company objectives, including mission and vision statements, operational objectives at the entity and functional levels, financial performance goals, and other objectives as appropriate, to serve as the basis for risk assessment activities and management communicated its objectives and any changes to those objectives to personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network security configurations are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.	Inspected the network diagram and security groups and associated inbound and outbound rules to determine that network security configurations were in place to limit inbound and outbound traffic to the environment to only what was necessary based on business justification, and all other traffic was specifically denied.	No exceptions noted.
		Production systems and resources are monitored and automated alerts are sent out personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalated per policy if necessary.	Inspected the monitoring tool configurations, the anti-malware software dashboard console, source code repository configurations, IDS configurations, firewall rule sets for a sample of production servers, and the anti-malware, source code repository, and IDS alert configurations and an example alert to determine that production systems and resources were monitored and automated alerts were sent out personnel based on pre-configured rules, and events were triaged to determine if they constituted an incident and escalated per policy if necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	Inspected the threat detection system and an example alert to determine that a threat detection system was in place to monitor web traffic and suspicious activity, and when anomalous traffic activity was identified, alerts were automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	No exceptions noted.
		A firewall is in place to protect public-facing web applications from outside threats.	Inspected the network diagram and the firewall configurations for the production environment to determine that a firewall was in place to protect public-facing web applications from outside threats.	No exceptions noted.
		An IDS is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected.	Inspected the network diagram and IDS configurations to determine that an IDS was in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and was configured to alert personnel when a potential intrusion was detected.	No 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.	The deployed anti-malware solution is kept current via automatic updates and configured to detect all known types of malware and to remove, block, or contain all known types of malware.	Inspected the anti-malware settings to determine that the deployed anti-malware solution was kept current via automatic updates and configured to detect all known types of malware and to remove, block, or contain all known types of malware.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The implemented anti-malware solutions are configured to perform real-time scans.	Inspected the anti-malware settings to determine that the implemented anti-malware solutions were configured to perform real-time scans.	No exceptions noted.
		Audit logs are enabled and active for system components and sensitive data in accordance with company policies.	Inspected the information security and logging and monitoring policies and procedures and network audit logging settings and an example audit log extract to determine that audit logs were enabled and active for system components and sensitive data in accordance with company policies.	No exceptions noted.
		The Company has source code repository to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts.	Inspected the source code repository configurations to determine that the Company had source code repository to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data could not be changed without generating alerts.	No exceptions noted.
		Anti-malware software is installed on company-managed devices.	Inspected the anti-malware software dashboard console to determine that anti-malware software was installed on company-managed devices.	No exceptions noted.
			Inspected the anti-malware settings for a sample of devices to determine that anti-malware software was installed on company-managed devices.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network security controls are in place to restrict public access to remote server administration ports to authorized IP addresses or address ranges only.	Inspected the security groups and associated inbound and outbound rules to determine that network security controls were in place to restrict public access to remote server administration ports to authorized IP addresses or address ranges only.	No exceptions noted.
		The Company has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company.	Inspected the information security policies and procedures and logging and monitoring policies and procedures to determine that the Company had a documented policy that outlined requirements for audit logging and monitoring of system activity at the company.	No exceptions noted.
		Cloud resources are configured to deny public access.	Inspected the security groups and associated inbound and outbound rules to determine that cloud resources were configured to deny public access.	No exceptions noted.
		The Company provides external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer communications are responded to within defined SLAs.	Inquired of the VP, Security and IT Operations regarding customer support issues to determine that the company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident management and escalation policies and procedures to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.
			Inspected the supporting ticket for a sample of customer support issues to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	Testing of the control activity disclosed that there were no customer support issues during the review period.
		Network security configurations are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.	Inspected the network diagram and security groups and associated inbound and outbound rules to determine that network security configurations were in place to limit inbound and outbound traffic to the environment to only what was necessary based on business justification, and all other traffic was specifically denied.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production systems and resources are monitored and automated alerts are sent out personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalated per policy if necessary.	Inspected the monitoring tool configurations, the anti-malware software dashboard console, source code repository configurations, IDS configurations, firewall rule sets for a sample of production servers, and the anti-malware, source code repository, and IDS alert configurations and an example alert to determine that production systems and resources were monitored and automated alerts were sent out personnel based on pre-configured rules, and events were triaged to determine if they constituted an incident and escalated per policy if necessary.	No exceptions noted.
		A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	Inspected the threat detection system and an example alert to determine that a threat detection system was in place to monitor web traffic and suspicious activity, and when anomalous traffic activity was identified, alerts were automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	No exceptions noted.
		A firewall is in place to protect public-facing web applications from outside threats.	Inspected the network diagram and the firewall configurations for the production environment to determine that a firewall was in place to protect public-facing web applications from outside threats.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Internal communication channels are in place for employees to report failures, events, incidents, concerns, and other issues to company management.	Inspected the company's website, compliance automation software, code of conduct, internal communication channel and incident management and escalation policies and procedures to determine that internal communication channels were in place for employees to report failures, events, incidents, concerns, and other issues to company management.	No exceptions noted.
		An IDS is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected.	Inspected the network diagram and IDS configurations to determine that an IDS was in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and was configured to alert personnel when a potential intrusion was detected.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	The Company has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan is reviewed at least annually and updated as needed according to lessons learned from previous incidents and industry developments.	Inspected the incident response policies and procedures, including the revision history, to determine that the Company had a documented incident response plan that outlined roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents, and the incident response plan was reviewed at least annually and updated as needed according to lessons learned from previous incidents and industry developments.	No exceptions noted.
		The Company evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	Inquired of the VP, Security and IT Operations regarding security incidents to determine that the Company evaluated security events to determine if they constituted an incident, and incidents were assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident response policies and procedures to determine that the Company evaluated security events to determine if they constituted an incident, and incidents were assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that the Company evaluated security events to determine if they constituted an incident, and incidents were assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	Testing of the control activity disclosed that there were no incidents during the review period.
		The Company has identified and documented roles and responsibilities for incident management.	Inspected the organization chart, job descriptions for a sample of job roles and incident response policies and procedures to determine that the Company had identified and documented roles and responsibilities for incident management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company provides external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer communications are responded to within defined SLAs.	Inquired of the VP, Security and IT Operations regarding customer support issues to determine that the company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.
			Inspected the incident management and escalation policies and procedures to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.
			Inspected the supporting ticket for a sample of customer support issues to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	Testing of the control activity disclosed that there were no customer support issues during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Internal communication channels are in place for employees to report failures, events, incidents, concerns, and other issues to company management.	Inspected the company's website, compliance automation software, code of conduct, internal communication channel and incident management and escalation policies and procedures to determine that internal communication channels were in place for employees to report failures, events, incidents, concerns, and other issues to company management.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
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.	The Company provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.	Inquired of the VP, Security and IT Operations regarding critical security incidents to determine that the Company provided communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident response policies and procedures to determine that the Company provided communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of critical security incidents to determine that the Company provided communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.	Testing of the control activity disclosed that no critical security incidents occurred during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan is reviewed at least annually and updated as needed according to lessons learned from previous incidents and industry developments.	Inspected the incident response policies and procedures, including the revision history, to determine that the Company had a documented incident response plan that outlined roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents, and the incident response plan was reviewed at least annually and updated as needed according to lessons learned from previous incidents and industry developments.	No exceptions noted.
		The Company evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	Inquired of the VP, Security and IT Operations regarding security incidents to determine that the Company evaluated security events to determine if they constituted an incident, and incidents were assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident response policies and procedures to determine that the Company evaluated security events to determine if they constituted an incident, and incidents were assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that the Company evaluated security events to determine if they constituted an incident, and incidents were assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	Testing of the control activity disclosed that there were no incidents during the review period.
		The Company has identified and documented roles and responsibilities for incident management.	Inspected the organization chart, job descriptions for a sample of job roles and incident response policies and procedures to determine that the Company had identified and documented roles and responsibilities for incident management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company provides external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer communications are responded to within defined SLAs.	Inquired of the VP, Security and IT Operations regarding customer support issues to determine that the company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.
			Inspected the incident management and escalation policies and procedures to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.
			Inspected the supporting ticket for a sample of customer support issues to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	Testing of the control activity disclosed that there were no customer support issues during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Internal communication channels are in place for employees to report failures, events, incidents, concerns, and other issues to company management.	Inspected the company's website, compliance automation software, code of conduct, internal communication channel and incident management and escalation policies and procedures to determine that internal communication channels were in place for employees to report failures, events, incidents, concerns, and other issues to company management.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The Company has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan is reviewed at least annually and updated as needed according to lessons learned from previous incidents and industry developments.	Inspected the incident response policies and procedures, including the revision history, to determine that the Company had a documented incident response plan that outlined roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents, and the incident response plan was reviewed at least annually and updated as needed according to lessons learned from previous incidents and industry developments.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has a defined business continuity plan that outlines strategies for maintaining operations during a disruption.	Inspected the business continuity plan to determine that the Company had a defined business continuity plan that outlined strategies for maintaining operations during a disruption.	No exceptions noted.
		The Company has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	Inspected the disaster recovery plans to determine that the Company had a documented disaster recovery plan that outlined roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	No exceptions noted.
		The Company conducts tests of the disaster recovery plans at least annually. Results and lessons learned are documented, and updates to the plans are made as necessary.	Inspected the completed disaster recovery test results to determine that the Company conducted tests of the disaster recovery plans at least annually, and the results and lessons learned were documented, and updates to the plans were made as necessary.	No exceptions noted.
		The Company has identified and documented roles and responsibilities for incident management.	Inspected the organization chart, job descriptions for a sample of job roles and incident response policies and procedures to determine that the Company had identified and documented roles and responsibilities for incident management.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**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.	The Company uses a version control system to manage source code, change documentation and tracking, release labeling, and other change management tasks.	Inspected the source code repository configurations to determine that the Company used a version control system to manage source code, change documentation and tracking, release labeling, and other change management tasks.	No exceptions noted.
		The Company has source code repository to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts.	Inspected the source code repository configurations to determine that the Company had source code repository to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data could not be changed without generating alerts.	No exceptions noted.
		The Company has a documented a policy that describes the requirements for managing changes across the organization, including changes to infrastructure, systems, and applications.	Inspected the change management policies and procedures to determine that the Company had a documented a policy that described the requirements for managing changes across the organization, including changes to infrastructure, systems, and applications.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Access to make changes in production environments is restricted to authorized personnel in accordance with segregation of duties principles and the company's documented policies and procedures.	Inquired of the VP, Security and IT Operations regarding the ability to migrate changes into the production environment to determine that access to make changes in production environments was restricted to authorized personnel in accordance with segregation of duties principles and the company's documented policies and procedures.	No exceptions noted.
			Inspected the change management policies and procedures and list of users with the ability to deploy changes into the environment to determine that access to make changes in internal environments was restricted to authorized personnel in accordance with segregation of duties principles and the company's documented policies and procedures.	No exceptions noted.
		Pre-production environments are separated from production environments and the separation is enforced with access controls.	Inspected the separate development, QA and production environments to determine that pre-production environments were separated from production environments and the separation was enforced with access controls.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company communicates system changes via release notes or change log via periodic communications.	Inspected the internal communication changes and the supporting e-mail communications to external users to determine that the Company communicated system changes via release notes or change log via periodic communications.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in implementing changes in an emergency situation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The Company has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	Inspected the risk assessment policies and procedures to determine that the Company had defined and documented a process for risk assessment and risk management that outlined the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	No exceptions noted.
		The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented.	Inspected the completed risk assessment to determine that the Company conducted risks assessments annually as required by company policy and compliance requirements, the risk assessment included consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk, a risk owner was assigned to each risk, every risk was assigned a risk treatment option, and the results of the risk assessment were documented.	No exceptions noted.
		Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected the completed risk assessment to determine that management had documented a risk treatment plan to formally manage risks identified in risk assessment activities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The Company has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	Inspected the risk assessment policies and procedures to determine that the Company had defined and documented a process for risk assessment and risk management that outlined the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	No exceptions noted.
		The Company maintains cybersecurity insurance to mitigate the financial impact of security incidents and business disruptions.	Inspected the cybersecurity insurance documentation to determine that the Company maintained cybersecurity insurance to mitigate the financial impact of security incidents and business disruptions.	No exceptions noted.
		The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented.	Inspected the completed risk assessment to determine that the Company conducted risks assessments annually as required by company policy and compliance requirements, the risk assessment included consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk, a risk owner was assigned to each risk, every risk was assigned a risk treatment option, and the results of the risk assessment were documented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle.	Inspected the vendor management policies and procedures to determine that the Company had a documented policy that outlined requirements for managing vendor and third-party relationships through their entire life cycle.	No exceptions noted.
		Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected the completed risk assessment to determine that management had documented a risk treatment plan to formally manage risks identified in risk assessment activities.	No exceptions noted.
		The Company performs due diligence activities prior to engaging with a new service provider or vendor. Results of the due diligence activities including action items are documented.	Inspected the vendor listing and completed supplier evaluation form for a sample of third-parties to determine that the Company performed due diligence activities prior to engaging with a new service provider or vendor, and the results of the due diligence activities including action items were documented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company maintains a third-party register that includes a complete and accurate list of third-parties, relationship owners, description for each of the services provided, risk ratings, results of third-party risk management activities, etc. The Company executes agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outline the responsibilities of each vendor or service provider.	Inspected the third-party register to determine that the Company maintained a third-party register that included a complete and accurate list of third-parties, relationship owners, description for each of the services provided, risk ratings, results of third-party risk management activities, etc., and the Company executed agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outlined the responsibilities of each vendor or service provider.	No exceptions noted.
			Inspected the third-party agreement for a sample of third-parties to determine that the Company maintained a third-party register that included a complete and accurate list of third-parties, relationship owners, description for each of the services provided, risk ratings, results of third-party risk management activities, etc., and the Company executed agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outlined the responsibilities of each vendor or service provider.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, are documented.	Inspected the compliance reports and associated review documentation for a sample of third-parties to determine that the Company obtained and reviewed compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, were documented.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(1)(i)	Security management process: Implement policies and procedures to prevent, detect, contain and correct security violations.	The company has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloguing, and assigning risk ratings to vulnerabilities to prioritize remediation efforts.	Inspected the vulnerability management policies and procedures to determine that the company had a defined policy that established requirements for vulnerability management across the organization, including monitoring, cataloguing, and assigning risk ratings to vulnerabilities to prioritize remediation efforts.	No exceptions noted.
		An external penetration test of production environments is performed by an independent third-party annually. Results are reviewed by management and vulnerabilities are tracked to resolution in accordance with company policies.	Inspected the completed penetration test results and associated resolution documentation to determine that an external penetration test of production environments was performed by an independent third-party annually and the results were reviewed by management and vulnerabilities were tracked to resolution in accordance with company policies.	No exceptions noted.
		The deployed anti-malware solution is kept current via automatic updates and configured to detect all known types of malware and to remove, block, or contain all known types of malware.	Inspected the anti-malware settings to determine that the deployed anti-malware solution was kept current via automatic updates and configured to detect all known types of malware and to remove, block, or contain all known types of malware.	No exceptions noted.
		The implemented anti-malware solutions are configured to perform real-time scans.	Inspected the anti-malware settings to determine that the implemented anti-malware solutions were configured to perform real-time scans.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has configured account lockout duration following a set number of invalid authentication attempts to a minimum of 60 minutes or until the identity of the user is confirmed.	Inspected the network account lockout duration settings to determine that the Company had configured account lockout duration following a set number of invalid authentication attempts to a minimum of 60 minutes or until the identity of the user was confirmed.	No exceptions noted.
		Audit logs are enabled and active for system components and sensitive data in accordance with company policies.	Inspected the information security and logging and monitoring policies and procedures and network audit logging settings and an example audit log extract to determine that audit logs were enabled and active for system components and sensitive data in accordance with company policies.	No exceptions noted.
		The Company has source code repository to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts.	Inspected the source code repository configurations to determine that the Company had source code repository to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data could not be changed without generating alerts.	No exceptions noted.
		Anti-malware software is installed on company-managed devices.	Inspected the anti-malware software dashboard console to determine that anti-malware software was installed on company-managed devices.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the anti-malware settings for a sample of devices to determine that anti-malware software was installed on company-managed devices.	No exceptions noted.
		The Company has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company.	Inspected the information security policies and procedures and logging and monitoring policies and procedures to determine that the Company had a documented policy that outlined requirements for audit logging and monitoring of system activity at the company.	No exceptions noted.
		The Company provides external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer communications are responded to within defined SLAs.	Inquired of the VP, Security and IT Operations regarding customer support issues to determine that the company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.
			Inspected the incident management and escalation policies and procedures to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting ticket for a sample of customer support issues to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	Testing of the control activity disclosed that there were no customer support issues during the review period.
		Production systems and resources are monitored and automated alerts are sent out personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalated per policy if necessary.	Inspected the monitoring tool configurations, the anti-malware software dashboard console, source code repository configurations, IDS configurations, firewall rule sets for a sample of production servers, and the anti-malware, source code repository, and IDS alert configurations and an example alert to determine that production systems and resources were monitored and automated alerts were sent out personnel based on pre-configured rules, and events were triaged to determine if they constituted an incident and escalated per policy if necessary.	No exceptions noted.
		A firewall is in place to protect public-facing web applications from outside threats.	Inspected the network diagram and the firewall configurations for the production environment to determine that a firewall was in place to protect public-facing web applications from outside threats.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		An IDS is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected.	Inspected the network diagram and IDS configurations to determine that an IDS was in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and was configured to alert personnel when a potential intrusion was detected.	No exceptions noted.
164.308 (a)(1)(ii)(A)	Risk analysis: Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.	The Company has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	Inspected the risk assessment policies and procedures to determine that the Company had defined and documented a process for risk assessment and risk management that outlined the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	No exceptions noted.
		The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented.	Inspected the completed risk assessment to determine that the Company conducted risks assessments annually as required by company policy and compliance requirements, the risk assessment included consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk, a risk owner was assigned to each risk, every risk was assigned a risk treatment option, and the results of the risk assessment were documented.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(1)(ii)(B)	Risk management: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a). Factors identified in §164.306 include: • The size, complexity, capability of the covered entity • The covered entity's technical infrastructure • The costs of security measures • The probability and criticality of potential risks to ePHI	The Company has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle.	Inspected the vendor management policies and procedures to determine that the Company had a documented policy that outlined requirements for managing vendor and third-party relationships through their entire life cycle.	No exceptions noted.
		Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected the completed risk assessment to determine that management had documented a risk treatment plan to formally manage risks identified in risk assessment activities.	No exceptions noted.
		The company has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloguing, and assigning risk ratings to vulnerabilities to prioritize remediation efforts.	Inspected the vulnerability management policies and procedures to determine that the company had a defined policy that established requirements for vulnerability management across the organization, including monitoring, cataloguing, and assigning risk ratings to vulnerabilities to prioritize remediation efforts.	No exceptions noted.
		An external penetration test of production environments is performed by an independent third-party annually. Results are reviewed by management and vulnerabilities are tracked to resolution in accordance with company policies.	Inspected the completed penetration test results and associated resolution documentation to determine that an external penetration test of production environments was performed by an independent third-party annually and the results were reviewed by management and vulnerabilities were tracked to resolution in accordance with company policies.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The deployed anti-malware solution is kept current via automatic updates and configured to detect all known types of malware and to remove, block, or contain all known types of malware.	Inspected the anti-malware settings to determine that the deployed anti-malware solution was kept current via automatic updates and configured to detect all known types of malware and to remove, block, or contain all known types of malware.	No exceptions noted.
		The implemented anti-malware solutions are configured to perform real-time scans.	Inspected the anti-malware settings to determine that the implemented anti-malware solutions were configured to perform real-time scans.	No exceptions noted.
		The Company has source code repository to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts.	Inspected the source code repository configurations to determine that the Company had source code repository to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data could not be changed without generating alerts.	No exceptions noted.
		Anti-malware software is installed on company-managed devices.	Inspected the anti-malware software dashboard console to determine that anti-malware software was installed on company-managed devices.	No exceptions noted.
			Inspected the anti-malware settings for a sample of devices to determine that anti-malware software was installed on company-managed devices.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network security controls are in place to restrict public access to remote server administration ports to authorized IP addresses or address ranges only.	Inspected the security groups and associated inbound and outbound rules to determine that network security controls were in place to restrict public access to remote server administration ports to authorized IP addresses or address ranges only.	No exceptions noted.
		Cloud resources are configured to deny public access.	Inspected the security groups and associated inbound and outbound rules to determine that cloud resources were configured to deny public access.	No exceptions noted.
		Network security configurations are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.	Inspected the network diagram and security groups and associated inbound and outbound rules to determine that network security configurations were in place to limit inbound and outbound traffic to the environment to only what was necessary based on business justification, and all other traffic was specifically denied.	No exceptions noted.
		A firewall is in place to protect public-facing web applications from outside threats.	Inspected the network diagram and the firewall configurations for the production environment to determine that a firewall was in place to protect public-facing web applications from outside threats.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		An IDS is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected.	Inspected the network diagram and IDS configurations to determine that an IDS was in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and was configured to alert personnel when a potential intrusion was detected.	No exceptions noted.
164.308 (a)(1)(ii)(C)	Sanction policy: Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	The Company has a defined disciplinary sanctions process to be enacted when a member of the workforce violates the Company's policies or causes a security or privacy incident. Management retains documentation of instances when the disciplinary process was enacted.	Inquired of the VP, Security and IT Operations regarding the disciplinary process to determine that the company had a defined disciplinary process to be enacted when a member of the workforce violated the company's policies or caused a security or privacy incident, and management retained documentation of instances when the disciplinary process was enacted.	No exceptions noted.
			Inspected the code of conduct to determine that the Company had a defined disciplinary sanctions process to be enacted when a member of the workforce violated the Company's policies or caused a security or privacy incident. Management retained documentation of instances when the disciplinary process was enacted.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the HR records to determine that the Company had a defined disciplinary sanctions process to be enacted when a member of the workforce violated the Company's policies or caused a security or privacy incident, and management retained documentation of instances when the disciplinary process was enacted.	Testing of the control activity disclosed that there were no instances where a member of the workforce violated the company's policies or caused a security or privacy incident during the review period.
164.308 (a)(1)(ii)(D)	Information system activity review: Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Audit logs are enabled and active for system components and sensitive data in accordance with company policies.	Inspected the information security and logging and monitoring policies and procedures and network audit logging settings and an example audit log extract to determine that audit logs were enabled and active for system components and sensitive data in accordance with company policies.	No exceptions noted.
		The Company has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company.	Inspected the information security policies and procedures and logging and monitoring policies and procedures to determine that the Company had a documented policy that outlined requirements for audit logging and monitoring of system activity at the company.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(2)	Assigned security responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	Inspected the risk management policies and procedures to determine that management had defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	No exceptions noted.
164.308 (a)(3)(i)	Workforce security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under the Information Access Management standard and to prevent those who do not have appropriate access from obtaining access to ePHI. Policies and procedures should include Authorization and/or Supervision procedures, Workforce Clearance Procedure, and Termination Procedures.	The Company has developed and documented a policy that outlines requirements for access control.	Inspected the system access control policies and procedures to determine that the Company had developed and documented a policy that outlined requirements for access control.	No exceptions noted.
		Management performs user access reviews to validate user accounts, including third-party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical access as necessary. Changes resulting from the review, if any, are documented and implemented.	Inspected the completed network user access review to determine that management performed user access reviews to validate user accounts, including third-party or vendor accounts, and their associated privileges remained appropriate, the review included validation of logical access as necessary, and changes resulting from the review, if any, were documented and implemented.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	Inspected the system access control policies and procedures, password policies and procedures and compliance automation software to determine that the Company had documented policies and procedures for authentication that were communicated to all personnel, and that these documents included guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	No exceptions noted.
		Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel.	Inquired of the VP, Security and IT Operations regarding privileged access to determine that administrative or privileged access to systems, resources, and functions was restricted to authorized personnel.	No exceptions noted.
			Inspected the network administrator listings and access rights to determine that administrative or privileged access to systems, resources, and functions was restricted to authorized personnel.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy.	Inspected the system access control policies and procedures, password policies and procedures, and authentication and password configurations for the network layer and the systems storing or maintaining ePHI to determine that the Company had a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems, and password requirements were enforced for all systems in accordance with company policy.	No exceptions noted.
		Access requests to information resources, including access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	Inspected the system access control policies and procedures, network, application, database, operating system user listings, and user access request ticket for a sample of new hires to determine that access requests to information resources, including access to systems and data, were documented and approved by management based on least privilege, need to know, and segregation of duties principles.	No exceptions noted.
		Authentication to systems requires the use of unique identities.	Inspected the network user listings and access rights to determine that authentication to systems required the use of unique identities.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(3)(ii)(A)	Authorization and/or supervision: Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	The Company has developed and documented a policy that outlines requirements for access control.	Inspected the system access control policies and procedures to determine that the Company had developed and documented a policy that outlined requirements for access control.	No exceptions noted.
		The Company has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	Inspected the system access control policies and procedures, password policies and procedures and compliance automation software to determine that the Company had documented policies and procedures for authentication that were communicated to all personnel, and that these documents included guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy.	Inspected the system access control policies and procedures, password policies and procedures, and authentication and password configurations for the network layer and the systems storing or maintaining ePHI to determine that the Company had a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems, and password requirements were enforced for all systems in accordance with company policy.	No exceptions noted.
		Access requests to information resources, including access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	Inspected the system access control policies and procedures, network, application, database, operating system user listings, and user access request ticket for a sample of new hires to determine that access requests to information resources, including access to systems and data, were documented and approved by management based on least privilege, need to know, and segregation of duties principles.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(3)(ii)(B)	Workforce clearance procedure: Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	The Company has developed and documented a policy that outlines requirements for access control.	Inspected the system access control policies and procedures to determine that the Company had developed and documented a policy that outlined requirements for access control.	No exceptions noted.
		Management performs user access reviews to validate user accounts, including third-party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical access as necessary. Changes resulting from the review, if any, are documented and implemented.	Inspected the completed network user access review to determine that management performed user access reviews to validate user accounts, including third-party or vendor accounts, and their associated privileges remained appropriate, the review included validation of logical access as necessary, and changes resulting from the review, if any, were documented and implemented.	No exceptions noted.
		The Company has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	Inspected the system access control policies and procedures, password policies and procedures and compliance automation software to determine that the Company had documented policies and procedures for authentication that were communicated to all personnel, and that these documents included guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel.	Inquired of the VP, Security and IT Operations regarding privileged access to determine that administrative or privileged access to systems, resources, and functions was restricted to authorized personnel.	No exceptions noted.
			Inspected the network administrator listings and access rights to determine that administrative or privileged access to systems, resources, and functions was restricted to authorized personnel.	No exceptions noted.
		The Company has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy.	Inspected the system access control policies and procedures, password policies and procedures, and authentication and password configurations for the network layer and the systems storing or maintaining ePHI to determine that the Company had a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems, and password requirements were enforced for all systems in accordance with company policy.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Access requests to information resources, including access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	Inspected the system access control policies and procedures, network, application, database, operating system user listings, and user access request ticket for a sample of new hires to determine that access requests to information resources, including access to systems and data, were documented and approved by management based on least privilege, need to know, and segregation of duties principles.	No exceptions noted.
		Authentication to systems requires the use of unique identities.	Inspected the network user listings and access rights to determine that authentication to systems required the use of unique identities.	No exceptions noted.
164.308 (a)(3)(ii)(C)	Termination procedures: Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) [the Workforce Clearance Procedure] of this section.	The Company has developed and documented a policy that outlines requirements for access control.	Inspected the system access control policies and procedures to determine that the Company had developed and documented a policy that outlined requirements for access control.	No exceptions noted.
		System access is revoked within one business day of effective termination date for terminated users.	Inspected the system access control policies and procedures, internal network access user listings, and user access revocation ticket for a sample of terminated employees to determine that system and physical access was revoked within one business day of effective termination date for terminated users.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.308 (a)(4)(i)	Information access management: Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of the Privacy Rule. Policies and procedures should include: Isolating Health Care Clearinghouse Functions, Access Authorization and Access Establishment and Modification.	Management maintains policies and procedures that ensure the authorization of access to ePHI and are consistent with the applicable requirements of the Privacy Rule.	Inspected the information security policies and procedures to determine that management maintained policies and procedures that ensured the authorization of access to ePHI and were consistent with the applicable requirements of the Privacy Rule.	No exceptions noted.
164.308 (a)(4)(ii)(A)	Isolating healthcare clearinghouse functions: If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.
164.308 (a)(4)(ii)(B)	Access authorization: Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.	The Company has developed and documented a policy that outlines requirements for access control.	Inspected the system access control policies and procedures to determine that the Company had developed and documented a policy that outlined requirements for access control.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	Inspected the system access control policies and procedures, password policies and procedures and compliance automation software to determine that the Company had documented policies and procedures for authentication that were communicated to all personnel, and that these documents included guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	No exceptions noted.
		The Company has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy.	Inspected the system access control policies and procedures, password policies and procedures, and authentication and password configurations for the network layer and the systems storing or maintaining ePHI to determine that the Company had a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems, and password requirements were enforced for all systems in accordance with company policy.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Access requests to information resources, including access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	Inspected the system access control policies and procedures, network, application, database, operating system user listings, and user access request ticket for a sample of new hires to determine that access requests to information resources, including access to systems and data, were documented and approved by management based on least privilege, need to know, and segregation of duties principles.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.308 (a)(4)(ii)(C)	Access establishment and modification: Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	The Company has developed and documented a policy that outlines requirements for access control.	Inspected the system access control policies and procedures to determine that the Company had developed and documented a policy that outlined requirements for access control.	No exceptions noted.
		Management performs user access reviews to validate user accounts, including third-party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical access as necessary. Changes resulting from the review, if any, are documented and implemented.	Inspected the completed network user access review to determine that management performed user access reviews to validate user accounts, including third-party or vendor accounts, and their associated privileges remained appropriate, the review included validation of logical access as necessary, and changes resulting from the review, if any, were documented and implemented.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	Inspected the system access control policies and procedures, password policies and procedures and compliance automation software to determine that the Company had documented policies and procedures for authentication that were communicated to all personnel, and that these documents included guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	No exceptions noted.
		The Company has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy.	Inspected the system access control policies and procedures, password policies and procedures, and authentication and password configurations for the network layer and the systems storing or maintaining ePHI to determine that the Company had a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems, and password requirements were enforced for all systems in accordance with company policy.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Access requests to information resources, including access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	Inspected the system access control policies and procedures, network, application, database, operating system user listings, and user access request ticket for a sample of new hires to determine that access requests to information resources, including access to systems and data, were documented and approved by management based on least privilege, need to know, and segregation of duties principles.	No exceptions noted.
		System access is revoked within one business day of effective termination date for terminated users.	Inspected the system access control policies and procedures, internal network access user listings, and user access revocation ticket for a sample of terminated employees to determine that system and physical access was revoked within one business day of effective termination date for terminated users.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(5)(i)	Security awareness and training: Implement a security awareness and training program for all members of the workforce (including management). Component of the Security Awareness and Training program should include Security Reminders, Protection Malicious Software, Log-in Monitoring and Password Management.	The Company has established training programs to help personnel gain awareness of information security best practices. Personnel are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary.	Inspected the information security policies and procedures and training completion certificates for a sample of new hires and current employees to determine that the Company had established training programs to help personnel gain awareness of information security best practices, personnel were required to complete the training during onboarding, and periodic refresher training is provided to personnel at least annually and as deemed necessary.	No exceptions noted.
164.308 (a)(5)(ii)(B)	Protection from malicious software: Procedures for guarding against, detecting, and reporting malicious software.	The company has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloguing, and assigning risk ratings to vulnerabilities to prioritize remediation efforts.	Inspected the vulnerability management policies and procedures to determine that the company had a defined policy that established requirements for vulnerability management across the organization, including monitoring, cataloguing, and assigning risk ratings to vulnerabilities to prioritize remediation efforts.	No exceptions noted.
		The deployed anti-malware solution is kept current via automatic updates and configured to detect all known types of malware and to remove, block, or contain all known types of malware.	Inspected the anti-malware settings to determine that the deployed anti-malware solution was kept current via automatic updates and configured to detect all known types of malware and to remove, block, or contain all known types of malware.	No exceptions noted.
		The implemented anti-malware solutions are configured to perform real-time scans.	Inspected the anti-malware settings to determine that the implemented anti-malware solutions were configured to perform real-time scans.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Anti-malware software is installed on company-managed devices.	Inspected the anti-malware software dashboard console to determine that anti-malware software was installed on company-managed devices.	No exceptions noted.
			Inspected the anti-malware settings for a sample of devices to determine that anti-malware software was installed on company-managed devices.	No exceptions noted.
164.308 (a)(5)(ii)(C)	Log-in monitoring: Procedures for monitoring log-in attempts and reporting discrepancies.	Audit logs are enabled and active for system components and sensitive data in accordance with company policies.	Inspected the information security and logging and monitoring policies and procedures and network audit logging settings and an example audit log extract to determine that audit logs were enabled and active for system components and sensitive data in accordance with company policies.	No exceptions noted.
		The Company has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company.	Inspected the information security policies and procedures and logging and monitoring policies and procedures to determine that the Company had a documented policy that outlined requirements for audit logging and monitoring of system activity at the company.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(5)(ii)(D)	Password management: Procedures for creating, changing, and safeguarding passwords.	Invalid authentication attempts are limited by locking out the user ID after not more than five failed attempts.	Inspected the network account lockout settings to determine that invalid authentication attempts were limited by locking out the user ID after not more than five failed attempts.	No exceptions noted.
		The Company has configured account lockout duration following a set number of invalid authentication attempts to a minimum of 60 minutes or until the identity of the user is confirmed.	Inspected the network account lockout duration settings to determine that the Company had configured account lockout duration following a set number of invalid authentication attempts to a minimum of 60 minutes or until the identity of the user was confirmed.	No exceptions noted.
		The Company has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	Inspected the system access control policies and procedures, password policies and procedures and compliance automation software to determine that the Company had documented policies and procedures for authentication that were communicated to all personnel, and that these documents included guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy.	Inspected the system access control policies and procedures, password policies and procedures, and authentication and password configurations for the network layer and the systems storing or maintaining ePHI to determine that the Company had a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems, and password requirements were enforced for all systems in accordance with company policy.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.308 (a)(6)(i)	Security incident procedures: Implement policies and procedures to address security incidents. Policies and procedures should include response reporting.	The Company provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.	Inquired of the VP, Security and IT Operations regarding critical security incidents to determine that the Company provided communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident response policies and procedures to determine that the Company provided communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of critical security incidents to determine that the Company provided communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.	Testing of the control activity disclosed that no critical security incidents occurred during the review period.
		The Company has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan is reviewed at least annually and updated as needed according to lessons learned from previous incidents and industry developments.	Inspected the incident response policies and procedures, including the revision history, to determine that the Company had a documented incident response plan that outlined roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents, and the incident response plan was reviewed at least annually and updated as needed according to lessons learned from previous incidents and industry developments.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	Inquired of the VP, Security and IT Operations regarding security incidents to determine that the Company evaluated security events to determine if they constituted an incident, and incidents were assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that the Company evaluated security events to determine if they constituted an incident, and incidents were assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that the Company evaluated security events to determine if they constituted an incident, and incidents were assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	Testing of the control activity disclosed that there were no incidents during the review period.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has identified and documented roles and responsibilities for incident management.	Inspected the organization chart, job descriptions for a sample of job roles and incident response policies and procedures to determine that the Company had identified and documented roles and responsibilities for incident management.	No exceptions noted.
		The Company provides external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer communications are responded to within defined SLAs.	Inquired of the VP, Security and IT Operations regarding customer support issues to determine that the company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.
			Inspected the incident management and escalation policies and procedures to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting ticket for a sample of customer support issues to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	Testing of the control activity disclosed that there were no customer support issues during the review period.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.308 (a)(6)(ii)	Response and reporting: Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	The Company provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.	Inquired of the VP, Security and IT Operations regarding critical security incidents to determine that the Company provided communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident response policies and procedures to determine that the Company provided communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of critical security incidents to determine that the Company provided communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.	Testing of the control activity disclosed that no critical security incidents occurred during the review period.
		The Company has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan is reviewed at least annually and updated as needed according to lessons learned from previous incidents and industry developments.	Inspected the incident response policies and procedures, including the revision history, to determine that the Company had a documented incident response plan that outlined roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents, and the incident response plan was reviewed at least annually and updated as needed according to lessons learned from previous incidents and industry developments.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	Inquired of the VP, Security and IT Operations regarding security incidents to determine that the Company evaluated security events to determine if they constituted an incident, and incidents were assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that the Company evaluated security events to determine if they constituted an incident, and incidents were assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that the Company evaluated security events to determine if they constituted an incident, and incidents were assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	Testing of the control activity disclosed that there were no incidents during the review period.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has identified and documented roles and responsibilities for incident management.	Inspected the organization chart, job descriptions for a sample of job roles and incident response policies and procedures to determine that the Company had identified and documented roles and responsibilities for incident management.	No exceptions noted.
		The Company provides external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer communications are responded to within defined SLAs.	Inquired of the VP, Security and IT Operations regarding customer support issues to determine that the company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.
			Inspected the incident management and escalation policies and procedures to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting ticket for a sample of customer support issues to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	Testing of the control activity disclosed that there were no customer support issues during the review period.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.308 (a)(7)(i)	Contingency plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI.	The Company has a defined business continuity plan that outlines strategies for maintaining operations during a disruption.	Inspected the business continuity plan to determine that the Company had a defined business continuity plan that outlined strategies for maintaining operations during a disruption.	No exceptions noted.
		The Company has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	Inspected the disaster recovery plans to determine that the Company had a documented disaster recovery plan that outlined roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company conducts tests of the disaster recovery plans at least annually. Results and lessons learned are documented, and updates to the plans are made as necessary.	Inspected the completed disaster recovery test results to determine that the Company conducted tests of the disaster recovery plans at least annually, and the results and lessons learned were documented, and updates to the plans were made as necessary.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.308 (a)(7)(ii)(A)	Data backup plan: Establish and implement procedures to create and maintain retrievable exact copies of ePHI.	The Company has a defined backup policy that establishes the requirements for backup information, software and systems.	Inspected the backup policies and procedures to determine that the Company had a defined backup policy that established the requirements for backup information, software and systems.	No exceptions noted.
		Backups of production data are performed at least daily and are configured to be retained in accordance with the retention periods established in company policies and procedures.	Inspected the backup policies and procedures, backup schedule and configurations for a sample of critical systems to determine that backups of production data were performed at least daily and were configured to be retained in accordance with the retention periods established in company policies and procedures.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the backup history log for a sample of days to determine that backups of production data were performed at least daily and were configured to be retained in accordance with the retention periods established in company policies and procedures.	No exceptions noted.
		Automated notifications are sent to personnel in the event of a backup failure. Backup failures are investigated and resolved by engineering personnel following company policies and procedures.	Inquired of the VP, Security and IT Operations regarding backup failures to determine that automated notifications were sent to personnel in the event of a backup failure, and backup failures were investigated and resolved by engineering personnel following company policies and procedures.	No exceptions noted.
			Inspected the backup policies and procedures to determine that automated notifications were sent to personnel in the event of a backup failure, and backup failures were investigated and resolved by engineering personnel following company policies and procedures.	No exceptions noted.
			Inspected the backup notification configurations and the associated resolution documentation for a sample of backup failures to determine that automated notifications were sent to personnel in the event of a backup failure, and backup failures were investigated and resolved by engineering personnel following company policies and procedures.	Testing of the control activity disclosed that there were no backup failures occurred during the review period.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(7)(ii)(B)	Disaster recovery plan: Establish (and implement as needed) procedures to restore any loss of data.	The Company tests the integrity and completeness of backed-up data at least annually.	Inspected the completed backup restoration test results to determine that the Company tested the integrity and completeness of backed-up data at least annually.	No exceptions noted.
		The Company has a defined business continuity plan that outlines strategies for maintaining operations during a disruption.	Inspected the business continuity plan to determine that the Company had a defined business continuity plan that outlined strategies for maintaining operations during a disruption.	No exceptions noted.
		The Company has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	Inspected the disaster recovery plans to determine that the Company had a documented disaster recovery plan that outlined roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	No exceptions noted.
		The Company conducts tests of the disaster recovery plans at least annually. Results and lessons learned are documented, and updates to the plans are made as necessary.	Inspected the completed disaster recovery test results to determine that the Company conducted tests of the disaster recovery plans at least annually, and the results and lessons learned were documented, and updates to the plans were made as necessary.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(7)(ii)(C)	Emergency Mode Operation Plan: Establish and implement procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.	The Company has a defined business continuity plan that outlines strategies for maintaining operations during a disruption.	Inspected the business continuity plan to determine that the Company had a defined business continuity plan that outlined strategies for maintaining operations during a disruption.	No exceptions noted.
		The Company has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	Inspected the disaster recovery plans to determine that the Company had a documented disaster recovery plan that outlined roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	No exceptions noted.
		The Company conducts tests of the disaster recovery plans at least annually. Results and lessons learned are documented, and updates to the plans are made as necessary.	Inspected the completed disaster recovery test results to determine that the Company conducted tests of the disaster recovery plans at least annually, and the results and lessons learned were documented, and updates to the plans were made as necessary.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.308 (a)(7)(ii)(D)	Testing and revision procedures: Implement procedures for periodic testing and revision of contingency plans.	The Company tests the integrity and completeness of backed-up data at least annually.	Inspected the completed backup restoration test results to determine that the Company tested the integrity and completeness of backed-up data at least annually.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has a defined business continuity plan that outlines strategies for maintaining operations during a disruption.	Inspected the business continuity plan to determine that the Company had a defined business continuity plan that outlined strategies for maintaining operations during a disruption.	No exceptions noted.
		The Company has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	Inspected the disaster recovery plans to determine that the Company had a documented disaster recovery plan that outlined roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	No exceptions noted.
		The Company conducts tests of the disaster recovery plans at least annually. Results and lessons learned are documented, and updates to the plans are made as necessary.	Inspected the completed disaster recovery test results to determine that the Company conducted tests of the disaster recovery plans at least annually, and the results and lessons learned were documented, and updates to the plans were made as necessary.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.308 (a)(7)(ii)(E)	Applications and data criticality analysis: Assess the relative criticality of specific applications and data in support of another contingency plan component.	The Company has established a data classification policy in order to identify the types of information stored or processed by the organization and the protection measures that are required for each.	Inspected the data classification policies and procedures to determine that the Company had established a data classification policy in order to identify the types of information stored or processed by the organization and the protection measures that were required for each.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	Inspected the risk assessment policies and procedures to determine that the Company had defined and documented a process for risk assessment and risk management that outlined the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	No exceptions noted.
		A centralized asset register is maintained for physical, cloud, and other assets that includes descriptive attributes for asset accountability such as owner, description, location, classification, and other information based on the type of asset. Processes are in place to maintain an updated inventory through manual reviews or automated mechanisms.	Inspected the inventory listing of system assets and components, including the revision history, and compliance automation software to determine that a centralized asset register was maintained for physical, cloud, and other assets that included descriptive attributes for asset accountability such as owner, description, location, classification, and other information based on the type of asset, and processes were in place to maintain an updated inventory through manual reviews or automated mechanisms.	No exceptions noted.
164.308 (a)(8)	Evaluation: Perform a periodic technical and nontechnical evaluation based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of ePHI, that establishes the extent to which an entity’s security policies and procedures meet the requirement.	The Company has a defined business continuity plan that outlines strategies for maintaining operations during a disruption.	Inspected the business continuity plan to determine that the Company had a defined business continuity plan that outlined strategies for maintaining operations during a disruption.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The company has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloguing, and assigning risk ratings to vulnerabilities to prioritize remediation efforts.	Inspected the vulnerability management policies and procedures to determine that the company had a defined policy that established requirements for vulnerability management across the organization, including monitoring, cataloguing, and assigning risk ratings to vulnerabilities to prioritize remediation efforts.	No exceptions noted.
		An external penetration test of production environments is performed by an independent third-party annually. Results are reviewed by management and vulnerabilities are tracked to resolution in accordance with company policies.	Inspected the completed penetration test results and associated resolution documentation to determine that an external penetration test of production environments was performed by an independent third-party annually and the results were reviewed by management and vulnerabilities were tracked to resolution in accordance with company policies.	No exceptions noted.
		The Company has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	Inspected the disaster recovery plans to determine that the Company had a documented disaster recovery plan that outlined roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company conducts tests of the disaster recovery plans at least annually. Results and lessons learned are documented, and updates to the plans are made as necessary.	Inspected the completed disaster recovery test results to determine that the Company conducted tests of the disaster recovery plans at least annually, and the results and lessons learned were documented, and updates to the plans were made as necessary.	No exceptions noted.
164.308 (b)(1)	Business associate contracts and other arrangements: A covered entity, in accordance with 164.306 [The Security Standards: General Rules], may permit a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with 164.314 [the Organization Requirements] that the business associate will appropriately safeguard the information.	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.
164.308 (b)(2)	A business associate may permit a business that is a subcontractor to create, receive, maintain, or transmit ePHI on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information.	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (b)(3)	Written contract or other arrangement: Document the satisfactory assurances required by paragraph (b)(1) or (b2) above of this section through a written or other arrangement with the business associate that meets the applicable requirements of 164.314(a) [the Organizational Requirements].	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicate: • The boundaries of the system • System commitments and requirements • Terms, conditions and responsibilities between the involved parties	Inquired of the VP, Security and IT Operations, regarding business associate agreements to determine that the entity maintained business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicated: • The boundaries of the system • System commitments and requirements • Terms, conditions and responsibilities between the involved parties Inspected the business associates agreement template and business associates agreement for a sample of business associates to determine that the entity maintained procedures to guide management in engaging in business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicated: • The boundaries of the system • System commitments and requirements • Terms, conditions and responsibilities between the involved parties	No exceptions noted. No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (b)(4)	Arrangement: Document the satisfactory assurances required by paragraph (b)(1) [the Business Associates Contracts and Other Arrangements] of this section through a written or other arrangement with the business associate that meets the applicable requirements of 164.314(a).	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicate: • The boundaries of the system • System commitments and requirements • Terms, conditions and responsibilities between the involved parties	Inquired of the VP, Security and IT Operations, regarding business associate agreements to determine that the entity maintained business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicated: • The boundaries of the system • System commitments and requirements • Terms, conditions and responsibilities between the involved parties Inspected the business associates agreement template and business associates agreement for a sample of business associates to determine that the entity maintained procedures to guide management in engaging in business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicated: • The boundaries of the system • System commitments and requirements • Terms, conditions and responsibilities between the involved parties	No exceptions noted. No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.310 (a)(1)	Facility access controls: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	This requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.310 (a)(2)(i)	Contingency operations: Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	The Company tests the integrity and completeness of backed-up data at least annually.	Inspected the completed backup restoration test results to determine that the Company tested the integrity and completeness of backed-up data at least annually.	No exceptions noted.
		The Company has a defined business continuity plan that outlines strategies for maintaining operations during a disruption.	Inspected the business continuity plan to determine that the Company had a defined business continuity plan that outlined strategies for maintaining operations during a disruption.	No exceptions noted.
		The Company has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	Inspected the disaster recovery plans to determine that the Company had a documented disaster recovery plan that outlined roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	No exceptions noted.
		The Company conducts tests of the disaster recovery plans at least annually. Results and lessons learned are documented, and updates to the plans are made as necessary.	Inspected the completed disaster recovery test results to determine that the Company conducted tests of the disaster recovery plans at least annually, and the results and lessons learned were documented, and updates to the plans were made as necessary.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.310 (a)(2)(ii)	Facility security plan: Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	This requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.310 (a)(2)(iii)	Access control and validation procedures: Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	This requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.310 (a)(2)(iv)	Maintenance records: Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	This requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.310 (b)	Workstation use: Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.	Procedures that specify the proper functions, processes, and appropriate environments of workstations that access ePHI are in place.	Observed the workstation areas within the facility to determine that procedures that specify the proper functions, processes, and appropriate environments of workstations that access ePHI were in place.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the access control policies and procedures to determine that procedures that specify the proper functions, processes, and appropriate environments of workstations that access ePHI were in place.	No exceptions noted.
164.310 (c)	Workstation security: Covered entities should implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.
164.310 (d)(1)	Device and media control: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.	This requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.310 (d)(2)(i)	Disposal: Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.	The company disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.	Inquired of the VP, Security and IT Operations regarding data disposal to determine that the company disposed of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.	No exceptions noted.
			Inspected the data retention policies and procedures to determine that the company disposed of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the destruction certificate for a sample of requests to dispose of data on hardware to determine that the Company disposed of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.	Testing of the control activity disclosed that no requests to dispose of data occurred during the review period.
		The Company has documented policies and procedures for erasure or destruction of information that has been identified for disposal.	Inspected the data retention policies and procedures to determine that the company had documented and implemented policies and procedures for erasure or destruction of information that has been identified for disposal.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.310 (d)(2)(ii)	Media re-use: Implement procedures for removal of ePHI from electronic media before the media are made available for re-use. Ensure that ePHI previously stored on electronic media cannot be accessed and reused. Identify removable media and their use. Ensure that ePHI is removed from reusable media before they are used to record new information.	The company disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.	Inquired of the VP, Security and IT Operations regarding data disposal to determine that the company disposed of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the data retention policies and procedures to determine that the company disposed of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.	No exceptions noted.
			Inspected the destruction certificate for a sample of requests to dispose of data on hardware to determine that the Company disposed of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.	Testing of the control activity disclosed that no requests to dispose of data occurred during the review period.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.310 (d)(2)(iii)	Accountability: Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	This requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.310 (d)(2)(iv)	Data backup and storage: Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.	The Company has a defined backup policy that establishes the requirements for backup information, software and systems.	Inspected the backup policies and procedures to determine that the Company had a defined backup policy that established the requirements for backup information, software and systems.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Backups of production data are performed at least daily and are configured to be retained in accordance with the retention periods established in company policies and procedures.	Inspected the backup policies and procedures, backup schedule and configurations for a sample of critical systems to determine that backups of production data were performed at least daily and were configured to be retained in accordance with the retention periods established in company policies and procedures.	No exceptions noted.
			Inspected the backup history log for a sample of days to determine that backups of production data were performed at least daily and were configured to be retained in accordance with the retention periods established in company policies and procedures.	No exceptions noted.
		Automated notifications are sent to personnel in the event of a backup failure. Backup failures are investigated and resolved by engineering personnel following company policies and procedures.	Inquired of the VP, Security and IT Operations regarding backup failures to determine that automated notifications were sent to personnel in the event of a backup failure, and backup failures were investigated and resolved by engineering personnel following company policies and procedures.	No exceptions noted.
			Inspected the backup policies and procedures to determine that automated notifications were sent to personnel in the event of a backup failure, and backup failures were investigated and resolved by engineering personnel following company policies and procedures.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the backup notification configurations and the associated resolution documentation for a sample of backup failures to determine that automated notifications were sent to personnel in the event of a backup failure, and backup failures were investigated and resolved by engineering personnel following company policies and procedures.	Testing of the control activity disclosed that there were no backup failures occurred during the review period.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.312 (a)(1)	Access control: Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4) [Information Access Management].	The Company has developed and documented a policy that outlines requirements for access control.	Inspected the system access control policies and procedures to determine that the Company had developed and documented a policy that outlined requirements for access control.	No exceptions noted.
		Management performs user access reviews to validate user accounts, including third-party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical access as necessary. Changes resulting from the review, if any, are documented and implemented.	Inspected the completed network user access review to determine that management performed user access reviews to validate user accounts, including third-party or vendor accounts, and their associated privileges remained appropriate, the review included validation of logical access as necessary, and changes resulting from the review, if any, were documented and implemented.	No exceptions noted.
		Invalid authentication attempts are limited by locking out the user ID after not more than five failed attempts.	Inspected the network account lockout settings to determine that invalid authentication attempts were limited by locking out the user ID after not more than five failed attempts.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	Inspected the system access control policies and procedures, password policies and procedures and compliance automation software to determine that the Company had documented policies and procedures for authentication that were communicated to all personnel, and that these documents included guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	No exceptions noted.
		Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel.	Inquired of the VP, Security and IT Operations regarding privileged access to determine that administrative or privileged access to systems, resources, and functions was restricted to authorized personnel.	No exceptions noted.
			Inspected the network administrator listings and access rights to determine that administrative or privileged access to systems, resources, and functions was restricted to authorized personnel.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy.	Inspected the system access control policies and procedures, password policies and procedures, and authentication and password configurations for the network layer and the systems storing or maintaining ePHI to determine that the Company had a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems, and password requirements were enforced for all systems in accordance with company policy.	No exceptions noted.
		Access requests to information resources, including access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	Inspected the system access control policies and procedures, network, application, database, operating system user listings, and user access request ticket for a sample of new hires to determine that access requests to information resources, including access to systems and data, were documented and approved by management based on least privilege, need to know, and segregation of duties principles.	No exceptions noted.
		System access is revoked within one business day of effective termination date for terminated users.	Inspected the system access control policies and procedures, internal network access user listings, and user access revocation ticket for a sample of terminated employees to determine that system and physical access was revoked within one business day of effective termination date for terminated users.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Authentication to systems requires the use of unique identities.	Inspected the network user listings and access rights to determine that authentication to systems required the use of unique identities.	No exceptions noted.
164.312 (a)(2)(i)	Unique user identification: Assign a unique name and/or number for identifying and tracking user identity. Ensure that system activity can be traced to a specific user.	The Company has developed and documented a policy that outlines requirements for access control.	Inspected the system access control policies and procedures to determine that the Company had developed and documented a policy that outlined requirements for access control.	No exceptions noted.
	Ensure that the necessary data is available in the system logs to support audit and other related business functions.	Invalid authentication attempts are limited by locking out the user ID after not more than five failed attempts.	Inspected the network account lockout settings to determine that invalid authentication attempts were limited by locking out the user ID after not more than five failed attempts.	No exceptions noted.
		The Company has configured account lockout duration following a set number of invalid authentication attempts to a minimum of 60 minutes or until the identity of the user is confirmed.	Inspected the network account lockout duration settings to determine that the Company had configured account lockout duration following a set number of invalid authentication attempts to a minimum of 60 minutes or until the identity of the user was confirmed.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	Inspected the system access control policies and procedures, password policies and procedures and compliance automation software to determine that the Company had documented policies and procedures for authentication that were communicated to all personnel, and that these documents included guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	No exceptions noted.
		Audit logs are enabled and active for system components and sensitive data in accordance with company policies.	Inspected the information security and logging and monitoring policies and procedures and network audit logging settings and an example audit log extract to determine that audit logs were enabled and active for system components and sensitive data in accordance with company policies.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy.	Inspected the system access control policies and procedures, password policies and procedures, and authentication and password configurations for the network layer and the systems storing or maintaining ePHI to determine that the Company had a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems, and password requirements were enforced for all systems in accordance with company policy.	No exceptions noted.
		Authentication to systems requires the use of unique identities.	Inspected the network user listings and access rights to determine that authentication to systems required the use of unique identities.	No exceptions noted.
		The Company has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company.	Inspected the information security policies and procedures and logging and monitoring policies and procedures to determine that the Company had a documented policy that outlined requirements for audit logging and monitoring of system activity at the company.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.312 (a)(2)(ii)	Emergency access procedure: Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.	The Company has a defined business continuity plan that outlines strategies for maintaining operations during a disruption.	Inspected the business continuity plan to determine that the Company had a defined business continuity plan that outlined strategies for maintaining operations during a disruption.	No exceptions noted.
		The Company has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	Inspected the disaster recovery plans to determine that the Company had a documented disaster recovery plan that outlined roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	No exceptions noted.
		The Company conducts tests of the disaster recovery plans at least annually. Results and lessons learned are documented, and updates to the plans are made as necessary.	Inspected the completed disaster recovery test results to determine that the Company conducted tests of the disaster recovery plans at least annually, and the results and lessons learned were documented, and updates to the plans were made as necessary.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.312 (a)(2)(iv)	Encryption and decryption: Implement a mechanism to encrypt and decrypt ePHI.	Data at rest is encrypted using strong cryptographic algorithms.	Inspected the encryption configurations for data at rest to determine that data at rest was encrypted using strong cryptographic algorithms.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Data in transit is encrypted using strong cryptographic algorithms.	Inspected the encryption configurations for data in transit to determine that data in transit was encrypted using strong cryptographic algorithms.	No exceptions noted.
		Remote access to production systems is only available through an encrypted connection.	Inspected the encryption configurations to determine that remote access to production systems was only available through an encrypted connection.	No exceptions noted.
164.312 (b)	Audit controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.	The Company has developed and documented a policy that outlines requirements for access control.	Inspected the system access control policies and procedures to determine that the Company had developed and documented a policy that outlined requirements for access control.	No exceptions noted.
		The Company has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	Inspected the system access control policies and procedures, password policies and procedures and compliance automation software to determine that the Company had documented policies and procedures for authentication that were communicated to all personnel, and that these documents included guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Audit logs are enabled and active for system components and sensitive data in accordance with company policies.	Inspected the information security and logging and monitoring policies and procedures and network audit logging settings and an example audit log extract to determine that audit logs were enabled and active for system components and sensitive data in accordance with company policies.	No exceptions noted.
		The Company has source code repository to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts.	Inspected the source code repository configurations to determine that the Company had source code repository to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data could not be changed without generating alerts.	No exceptions noted.
		The Company has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company.	Inspected the information security policies and procedures and logging and monitoring policies and procedures to determine that the Company had a documented policy that outlined requirements for audit logging and monitoring of system activity at the company.	No exceptions noted.
164.312 (c)(1)	Integrity: Implement policies and procedures to protect ePHI from improper alteration or destruction.	The Company has documented policies and procedures for erasure or destruction of information that has been identified for disposal.	Inspected the data retention policies and procedures to determine that the company had documented and implemented policies and procedures for erasure or destruction of information that has been identified for disposal.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has source code repository to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts.	Inspected the source code repository configurations to determine that the Company had source code repository to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data could not be changed without generating alerts.	No exceptions noted.
		Data at rest is encrypted using strong cryptographic algorithms.	Inspected the encryption configurations for data at rest to determine that data at rest was encrypted using strong cryptographic algorithms.	No exceptions noted.
		Data in transit is encrypted using strong cryptographic algorithms.	Inspected the encryption configurations for data in transit to determine that data in transit was encrypted using strong cryptographic algorithms.	No exceptions noted.
		Remote access to production systems is only available through an encrypted connection.	Inspected the encryption configurations to determine that remote access to production systems was only available through an encrypted connection.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.312 (c)(2)	Mechanisms to authenticate ePHI: Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	The Company has documented policies and procedures for erasure or destruction of information that has been identified for disposal.	Inspected the data retention policies and procedures to determine that the company had documented and implemented policies and procedures for erasure or destruction of information that has been identified for disposal.	No exceptions noted.
		The Company has source code repository to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts.	Inspected the source code repository configurations to determine that the Company had source code repository to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data could not be changed without generating alerts.	No exceptions noted.
		Data at rest is encrypted using strong cryptographic algorithms.	Inspected the encryption configurations for data at rest to determine that data at rest was encrypted using strong cryptographic algorithms.	No exceptions noted.
		Data in transit is encrypted using strong cryptographic algorithms.	Inspected the encryption configurations for data in transit to determine that data in transit was encrypted using strong cryptographic algorithms.	No exceptions noted.
		Remote access to production systems is only available through an encrypted connection.	Inspected the encryption configurations to determine that remote access to production systems was only available through an encrypted connection.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.312 (d)	Person or entity authentication: Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	The Company has developed and documented a policy that outlines requirements for access control.	Inspected the system access control policies and procedures to determine that the Company had developed and documented a policy that outlined requirements for access control.	No exceptions noted.
		Invalid authentication attempts are limited by locking out the user ID after not more than five failed attempts.	Inspected the network account lockout settings to determine that invalid authentication attempts were limited by locking out the user ID after not more than five failed attempts.	No exceptions noted.
		The Company has configured account lockout duration following a set number of invalid authentication attempts to a minimum of 60 minutes or until the identity of the user is confirmed.	Inspected the network account lockout duration settings to determine that the Company had configured account lockout duration following a set number of invalid authentication attempts to a minimum of 60 minutes or until the identity of the user was confirmed.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	Inspected the system access control policies and procedures, password policies and procedures and compliance automation software to determine that the Company had documented policies and procedures for authentication that were communicated to all personnel, and that these documents included guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	No exceptions noted.
		The Company has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy.	Inspected the system access control policies and procedures, password policies and procedures, and authentication and password configurations for the network layer and the systems storing or maintaining ePHI to determine that the Company had a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems, and password requirements were enforced for all systems in accordance with company policy.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Authentication to systems requires the use of unique identities.	Inspected the network user listings and access rights to determine that authentication to systems required the use of unique identities.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.312 (e)(1)	Transmission security: Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.	The Company has documented policies and procedures for erasure or destruction of information that has been identified for disposal.	Inspected the data retention policies and procedures to determine that the company had documented and implemented policies and procedures for erasure or destruction of information that has been identified for disposal.	No exceptions noted.
		Data in transit is encrypted using strong cryptographic algorithms.	Inspected the encryption configurations for data in transit to determine that data in transit was encrypted using strong cryptographic algorithms.	No exceptions noted.
		Remote access to production systems is only available through an encrypted connection.	Inspected the encryption configurations to determine that remote access to production systems was only available through an encrypted connection.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.312 (e)(2)(i)	Integrity controls: Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.	The Company has documented policies and procedures for erasure or destruction of information that has been identified for disposal.	Inspected the data retention policies and procedures to determine that the company had documented and implemented policies and procedures for erasure or destruction of information that has been identified for disposal.	No exceptions noted.
		Data in transit is encrypted using strong cryptographic algorithms.	Inspected the encryption configurations for data in transit to determine that data in transit was encrypted using strong cryptographic algorithms.	No exceptions noted.
		Remote access to production systems is only available through an encrypted connection.	Inspected the encryption configurations to determine that remote access to production systems was only available through an encrypted connection.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.312 (e)(2)(ii)	Encryption: Implement a mechanism to encrypt ePHI whenever deemed appropriate.	Data at rest is encrypted using strong cryptographic algorithms.	Inspected the encryption configurations for data at rest to determine that data at rest was encrypted using strong cryptographic algorithms.	No exceptions noted.
		Data in transit is encrypted using strong cryptographic algorithms.	Inspected the encryption configurations for data in transit to determine that data in transit was encrypted using strong cryptographic algorithms.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Remote access to production systems is only available through an encrypted connection.	Inspected the encryption configurations to determine that remote access to production systems was only available through an encrypted connection.	No exceptions noted.
		Policies and procedures are formally documented regarding the mechanisms used to encrypt ePHI.	Inspected the encryption policies and procedures to determine that policies and procedures were formally documented regarding the mechanisms used to encrypt ePHI.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.

ORGANIZATIONAL REQUIREMENTS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.314 (a)(1)	Business associate contracts or other arrangements: A covered entity is not in compliance with the standards in § 164.502(e) if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful - (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary."	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicate: • The boundaries of the system • System commitments and requirements • Terms, conditions and responsibilities between the involved parties	Inquired of the VP, Security and IT Operations, regarding business associate agreements to determine that the entity maintained business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicated: • The boundaries of the system • System commitments and requirements • Terms, conditions and responsibilities between the involved parties Inspected the business associates agreement template and business associates agreement for a sample of business associates to determine that the entity maintained procedures to guide management in engaging in business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicated: • The boundaries of the system • System commitments and requirements • Terms, conditions and responsibilities between the involved parties	No exceptions noted. No exceptions noted.

ORGANIZATIONAL REQUIREMENTS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.314 (a)(2)(i)	Business Associate Contracts: A business associate contract must provide that the business associate will: “Implement safeguards that protect the confidentiality, integrity, and availability of the electronic protected health; Report to the covered entity any security incident of which it becomes aware; Authorize termination of the contract, if the covered entity determines that the business associate has violated a material term of the contract.”	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicate: • The boundaries of the system • System commitments and requirements • Terms, conditions and responsibilities between the involved parties	Inquired of the VP, Security and IT Operations, regarding business associate agreements to determine that the entity maintained business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicated: • The boundaries of the system • System commitments and requirements • Terms, conditions and responsibilities between the involved parties Inspected the business associates agreement template and business associates agreement for a sample of business associates to determine that the entity maintained procedures to guide management in engaging in business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicated: • The boundaries of the system • System commitments and requirements • Terms, conditions and responsibilities between the involved parties	No exceptions noted. No exceptions noted.

ORGANIZATIONAL REQUIREMENTS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.314 (a)(2)(ii)	Other Arrangement: The Other Arrangements implementation specifications provide that when a covered entity and its business associate are both government entities, the covered entity may comply with the standard in either of two alternative ways: (1) if it enters into a memorandum of understanding (MOU) with the business associate and the MOU contains terms which accomplish the objectives of the Business Associate Contracts section of the Security Rule; or (2) if other law (including regulations adopted by the covered entity or its business associate) contain requirements applicable to the business associate that accomplish the objectives of the business associate contract.	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.
164.314 (b)(1)	Requirements for Group Health Plans: Except when the only ePHI disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii), or as authorized under §164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard ePHI created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.

ORGANIZATIONAL REQUIREMENTS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.314 (b)(2)	Implementation Specifications: The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to - (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and (iv) Report to the group health plan any security incident of which it becomes aware.	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.

ORGANIZATIONAL REQUIREMENTS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.316 (a)	Policies and Procedures: Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in 164.306(b)(2)(i), (ii), (iii), and (iv) [the Security Standards: General Rules, Flexibility of Approach]. This standard is not to be construed to permit or excuse an action that violates any other standard. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.	The entity creates and implements appropriate policies and procedures as required by applicable legislations, regulators, and customers.	Inspected the information security policies and procedures to determine that the entity created and implemented appropriate policies and procedures as required by applicable legislations, regulators, and customers.	No exceptions noted.
		Policies and procedures are reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.	Inspected the revision history of the information security policies and procedures and ePHI policies and procedures and compliance automation software to determine that policies and procedures were reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.	No exceptions noted.
164.316 (b)(1)	Documentation: Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	Policies and procedures are reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.	Inspected the revision history of the information security policies and procedures and ePHI policies and procedures and compliance automation software to determine that policies and procedures were reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.	No exceptions noted.
		Policies and procedures are appropriately retained for a minimum of six years from the date it was created or when it was last in effect, whichever is later.	Inspected the data retention and disposal policies and procedures to determine that policies and procedures were appropriately retained for a minimum of six years from the date when it was last in effect.	No exceptions noted.

ORGANIZATIONAL REQUIREMENTS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Policies and procedures are created and maintained in written and electronic form.	Inspected the entity's policies and procedures to determine that policies and procedures were created and maintained in written and electronic form.	No exceptions noted.
		HIPAA related incidents and events are documented in a ticketing system.	Inspected the incident management ticketing tool to determine that HIPAA related incidents and events were documented in a ticketing system.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.316 (b)(2)(i)	Time Limit: Retain the documentation required by paragraph (b) (1) of this section for 6 years for the date of its creation or the date when it last was in effect, whichever is later.	Policies and procedures are appropriately retained for a minimum of six years from the date it was created or when it was last in effect, whichever is later.	Inspected the data retention and disposal policies and procedures to determine that policies and procedures were appropriately retained for a minimum of six years from the date when it was last in effect.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.

ORGANIZATIONAL REQUIREMENTS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.316 (b)(2)(ii)	Availability: Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Policies and procedures are reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.	Inspected the revision history of the information security policies and procedures and ePHI policies and procedures and compliance automation software to determine that policies and procedures were reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.316 (b)(2)(iii)	Updates: Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.	Policies and procedures are reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.	Inspected the revision history of the information security policies and procedures and ePHI policies and procedures and compliance automation software to determine that policies and procedures were reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.	No exceptions noted.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.402	Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. (1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual. (ii) A use or disclosure of protected health information that does not include the identifiers listed at §164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.	Breach notification letters or e-mails are developed and prepared to be used during a breach of ePHI. Notification procedures include: • Notice to parties alerting them to breaches "without unreasonable delay," but no later than 60 days after discovery of the breach • Notice to covered entities when breach is discovered • Notice to the secretary of HHS and prominent media outlets about breaches involving more than 500 individual subject's records • Notice to next of kin about breaches involving parties who are deceased • Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity's response • Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches involving fewer than 500 patient records	Inquired of the VP, Security and IT Operations, regarding breach notifications to determine that breach notification letters or e-mails were developed and prepared to be used during a breach of ePHI. Notification procedures included: • Notice to parties alerting them to breaches "without unreasonable delay," but no later than 60 days after discovery of the breach • Notice to Covered Entities when breach was discovered • Notice to the secretary of HHS and prominent media outlets about breaches that involved more than 500 individual subject's records • Notice to next of kin about breaches that involved parties who were deceased • Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity's response *Continues on the next page.	No exceptions noted.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			• Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches that involved fewer than 500 patient records Inspected the breach notification policies and procedures to determine that procedures were in place to guide personnel in developing breach notification letters or e-mails to be used during a breach of ePHI. Notification procedures included: • Notice to parties alerting them to breaches "without unreasonable delay," but no later than 60 days after discovery of the breach • Notice to Covered Entities when breach was discovered • Notice to the secretary of HHS and prominent media outlets about breaches that involved more than 500 individual subject's records • Notice to next of kin about breaches that involved parties who were deceased *Continues on the next page.*	No exceptions noted.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			• Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity's response • Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches that involved fewer than 500 patient records Inspected the breach notification e-mail for a sample of breaches of ePHI to determine that breach notification letters or e-mails were developed and prepared to be used during a breach of ePHI. Notification procedures included: • Notice to parties alerting them to breaches "without unreasonable delay," but no later than 60 days after discovery of the breach • Notice to Covered Entities when breach was discovered • Notice to the secretary of HHS and prominent media outlets about breaches that involved more than 500 individual subject's records *Continues on the next page.*	Testing of the control activity disclosed that there were no breaches of ePHI during the review period.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			• Notice to next of kin about breaches that involved parties who were deceased • Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity's response • Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches that involved fewer than 500 patient records	
		Part of this requirement is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.404 (a)(1)	A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used or disclosed as a result of such breach.	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.404 (a)(2)	For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.
164.404 (b)	Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 days after discovery of a breach.	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.404 (c)(1)	Elements of the notification required by paragraph (a) of this section shall include to the extent possible: (A) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (B) a description of the types of unsecured protected health information that were involved in the breach (Such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); (C) any steps the individual should take to protect themselves from potential harm resulting from the breach; (D) a brief description of what the covered entity is doing to investigation the breach, to mitigate harm to individuals, and to protect against further breaches; and (E) contact procedures for individuals to ask questions or learn additional information which should include a toll-free number, an e-mail address, website, or postal address.	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.
164.404 (c)(2)	The notification required by paragraph (a) of this section shall be written in plain language.	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.404 (d)(1)(i)	The notification required by paragraph (a) shall be provided in the following form: Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as more information becomes available.	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.
164.404 (d)(1)(ii)	The notification required by paragraph (a) shall be provided in the following form: If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under §164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.404 (d)(2)	Substitute notice. In the case where there is insufficient or out-of-date contact information that precludes written notification to the individual under this paragraph (d)(1)(i) of this section, a substitute form of notice reasonable calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.
164.404 (d)(2)(i)	In a case where there is insufficient or out-of-date contact information for fewer than 10 individuals, then substitute notice may be provided by an alternative form of written notice, telephone or other means.	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.404 (d)(2)(ii)	In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) be in the form of either a conspicuous posting for a period of 90 days on the home page of the web site of the covered entity involved, or conspicuous notice in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) include a toll-free number that remains active for at least 90 days where an individual can learn whether the individual's secured protected health information may be included in the breach.	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.
164.404 (d)(3)	In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.406	§164.406(a) For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach, notify prominent media outlets serving the State or jurisdiction. (b) Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. (c) The content of the notification required by paragraph (a) shall meet the requirements of §164.404(c).	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.
164.408 (a)	A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in §164.404(a)(2), notify the Secretary.	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.
164.408 (b)	For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, expect as provided in §164.412, provide the notification required by paragraph (a) contemporaneously with the notice required by §164.404(a) and in the manner specified on the HHS web site.	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.408 (c)	For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches occurring during the preceding calendar year, in a manner specified on the HHS web site.	This requirement is not applicable based on the services rendered by the service organization. Refer to the 'Criteria Not Applicable to the System' section above for the explanation as to why the requirement is not applicable.	Not applicable.	Not applicable.
164.410 (a)(1)	A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.	Breach notification letters or e-mails are developed and prepared to be used during a breach of ePHI. Notification procedures include: • Notice to parties alerting them to breaches “without unreasonable delay,” but no later than 60 days after discovery of the breach • Notice to covered entities when breach is discovered • Notice to the secretary of HHS and prominent media outlets about breaches involving more than 500 individual subject’s records • Notice to next of kin about breaches involving parties who are deceased *Continues on the next page.*	Inquired of the VP, Security and IT Operations, regarding breach notifications to determine that breach notification letters or e-mails were developed and prepared to be used during a breach of ePHI. Notification procedures included: • Notice to parties alerting them to breaches “without unreasonable delay,” but no later than 60 days after discovery of the breach • Notice to Covered Entities when breach was discovered • Notice to the secretary of HHS and prominent media outlets about breaches that involved more than 500 individual subject’s records *Continues on the next page.*	No exceptions noted.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		• Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity's response • Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches involving fewer than 500 patient records	• Notice to next of kin about breaches that involved parties who were deceased • Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity's response • Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches that involved fewer than 500 patient records Inspected the breach notification policies and procedures to determine that procedures were in place to guide personnel in developing breach notification letters or e-mails to be used during a breach of ePHI. Notification procedures included: • Notice to parties alerting them to breaches "without unreasonable delay," but no later than 60 days after discovery of the breach • Notice to Covered Entities when breach was discovered *Continues on the next page.	No exceptions noted.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			• Notice to the secretary of HHS and prominent media outlets about breaches that involved more than 500 individual subject's records • Notice to next of kin about breaches that involved parties who were deceased • Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity's response • Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches that involved fewer than 500 patient records	

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the breach notification e-mail for a sample of breaches of ePHI to determine that breach notification letters or e-mails were developed and prepared to be used during a breach of ePHI. Notification procedures included: • Notice to parties alerting them to breaches "without unreasonable delay," but no later than 60 days after discovery of the breach • Notice to Covered Entities when breach was discovered • Notice to the secretary of HHS and prominent media outlets about breaches that involved more than 500 individual subject's records • Notice to next of kin about breaches that involved parties who were deceased *Continues on the next page.*	Testing of the control activity disclosed that there were no breaches of ePHI during the review period.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			• Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity's response • Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches that involved fewer than 500 patient records	
164.410 (a)(2)	(2) For the purposes of paragraph (1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).	The entity acknowledges responsibility for notifying affected parties in the event of a breach of unsecured protected health information.	Inquired of the VP, Security and IT Operations regarding breach notifications to determine that procedures were in place to outline the responsibility of the entity personnel for notifying affected parties in the event of a breach of unsecured protected health information. Inspected the breach notification policies and procedures to determine that procedures were in place to outline the responsibility of the entity personnel for notifying affected parties in the event of a breach of unsecured protected health information.	No exceptions noted. No exceptions noted.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the breach notification e-mail for a sample of breaches of ePHI to determine that the entity acknowledged responsibility for notifying affected parties in the event of a breach of unsecured protected health information.	Testing of the control activity disclosed that there were no breaches of ePHI during the review period.
164.410 (b)	Except as provided in §164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach.	The entity notifies affected parties of a breach of ePHI no later than sixty calendar days after the discovery of the breach.	Inquired of the VP, Security and IT Operations regarding breach notifications to determine that the entity notified affected parties of a breach of ePHI no later than sixty calendar days after the discovery of the breach.	No exceptions noted.
			Inspected the breach notification policies and procedures to determine that the entity maintained procedures to guide personnel in notifying affected parties of a breach of ePHI no later than sixty (60) calendar days after the discovery of the breach.	No exceptions noted.
			Inspected the breach notification e-mail for a sample of breaches of ePHI to determine that the entity maintained procedures to guide personnel in notifying affected parties of a breach of ePHI no later than sixty (60) calendar days after the discovery of the breach.	Testing of the control activity disclosed that there were no breaches of ePHI during the review period.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.410 (c)(1)	The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been accessed, acquired, used or disclosure during the breach.	The identification of each individual whose unsecured ePHI has been accessed during the breach is disclosed during notification procedures.	Inquired of the VP, Security and IT Operations regarding breaches of ePHI to determine that the identification of each individual whose unsecured ePHI has been accessed during the breach was disclosed during the notification procedures.	No exceptions noted.
			Inspected the breach notification policies and procedures to determine that procedures were in place to guide personnel in disclosing the identification of each individual whose unsecured ePHI was accessed during the breach.	No exceptions noted.
			Inspected the breach notification e-mail for a sample of breaches of ePHI to determine that the identification of each individual whose unsecured ePHI has been accessed during the breach was disclosed during notification procedures.	Testing of the control activity disclosed that there were no breaches of ePHI during the review period.
164.410 (c)(2)	A business associate shall provide the covered entity with any other information that the covered entity is required to include in the notification to the individual under §164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.	Management provides the covered entity with any information that the covered entity is required to include in the notification to the individual at the time of the breach and as soon as it is available.	Inquired of the VP, Security and IT Operations regarding breach notifications to determine that management provided the covered entity with any information that the covered entity was required to include in the notification to the individual at the time of the breach and as soon as it was available.	No exceptions noted.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the breach notification policies and procedures to determine that procedures were in place to guide management in providing the covered entity with any information that the covered entity was required to include in the notification to the individual at the time of the breach and as soon as it was available.	No exceptions noted.
			Inspected the breach notification e-mail for a sample of breaches of ePHI to determine that management provided the covered entity with any information that the covered entity was required to include in the notification to the individual at the time of the breach and as soon as it was available.	Testing of the control activity disclosed that there were no breaches of ePHI during the review period.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.412	If a law enforcement official states to a covered entity or business associate that a notification, notice or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.	The entity refrains from, or delays notifying HHS personnel, the covered entity, or other required persons following the discovery of a breach of unsecured protected health information when required by law.	Inspected the breach notification policies and procedures to determine that the entity maintained procedures to guide personnel in refraining from, or delaying notification to the HHS personnel, the covered entity, or other required persons following the discovery of a breach of unsecured protected health information when required by law.	No exceptions noted.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.414	Administrative requirements and burden of proof: (a) Covered entity is required to comply with the administrative requirements of § 164.530(b), (d), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart. (b) In the event of a use or disclosure in violation of subpart E, the covered entity or business associate; as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosures did not constitute a breach as defined at §164.402. See §164.530 for definition of breach.	The entity acknowledges responsibility for notifying affected parties in the event of a breach of unsecured protected health information.	Inquired of the VP, Security and IT Operations regarding breach notifications to determine that procedures were in place to outline the responsibility of the entity personnel for notifying affected parties in the event of a breach of unsecured protected health information. Inspected the breach notification policies and procedures to determine that procedures were in place to outline the responsibility of the entity personnel for notifying affected parties in the event of a breach of unsecured protected health information. Inspected the breach notification e-mail for a sample of breaches of ePHI to determine that the entity acknowledged responsibility for notifying affected parties in the event of a breach of unsecured protected health information.	No exceptions noted. No exceptions noted. Testing of the control activity disclosed that there were no breaches of ePHI during the review period.

SECTION 5

OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results	Management's Response
CC1.1 CC1.4	Background checks are conducted on eligible personnel prior to hire as permitted by local laws.	Inspected the completed background check for a sample of new hires to determine that background checks were conducted on eligible personnel prior to hire as permitted by local laws.	Testing of the control activity disclosed that background check was not conducted in a timely manner for one of one new hire sampled.	This is noted by the Glooko team and has been addressed since the end of the review period.