Cassidy, Inc.

Type 2 Attestation (AT-C 105, AT-C 205 and AT-C 315) HIPAA/HITECH 2021

Cassidy Platform

For the Period April 18, 2026 – July 18, 2026

Advantage PARTNERS

Table of Contents

SECTION I: INDEPENDENT SERVICE AUDITOR'S REPORT 5
SECTION II: MANAGEMENT'S ASSERTION 10
SECTION III: DESCRIPTION OF THE SYSTEM 13
SECTION IV: DESCRIPTION OF CRITERIA, SERVICE AUDITOR TESTING 28

Executive Summary

Cassidy, Inc. - Cassidy Platform

Scope	Cassidy Platform
Period of Examination	For the Period April 18, 2026 – July 18, 2026
Subservice Providers	Amazon Web Services (AWS), Microsoft Azure (Azure) and Railway
Opinion Result	Unqualified
Testing Exceptions	No Exceptions Noted
Complementary Subservice Organization Controls	Yes – See **Page 24**
Complementary User Entity Controls	Yes – See **Page 26**

Section I: Independent Service Auditor's Report



Section I: Independent Service Auditor's Report

To: Management of Cassidy, Inc.

Scope

We have examined Cassidy, Inc.'s ("Cassidy" or the "Service Organization") description of its health information security program for the Cassidy Platform System listed in **Section III** (the "description"), and its health information security program governing the Cassidy Platform System compliance with applicable requirements 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 ("HIPAA/HITECH requirements"). Cassidy's management is responsible for its assertion. Our responsibility is to express an opinion about Cassidy's compliance with the specified requirements based on our examination.

The Service Organization uses subservice organizations listed in **Section III** to support its overall system. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Cassidy, to achieve Cassidy's service commitments and system requirements based on the applicable HIPAA/HITECH requirements. The description presents Cassidy's controls, the applicable HIPAA/HITECH requirements, and the complementary subservice organization controls assumed in the design of Cassidy'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.

Service Organization's Responsibilities

The Service Organization 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 Service Organization's service commitments and system requirements were achieved. The Service Organization has provided the accompanying assertion, "Management's Assertion" in **Section II**, ("assertion") about the description and the suitability of design and operating

effectiveness of controls stated therein. The Service Organization 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 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 Responsibility

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence supporting the fairness of the presentation of the description and the design of Cassidy's health information security program for the Cassidy Platform System and performing such other procedures as we considered necessary in the circumstances. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion about compliance with the specified requirements is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about whether management's assertion is fairly stated, in all material respects. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. 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 those 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;
- 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 HIPAA/HITECH requirements;
- Evaluating the overall presentation of the description.

Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA. We applied the statements on quality control standards established by the AICPA, and accordingly, maintain a comprehensive system of quality control.

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 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 our tests are listed in **Section IV** of this report.

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

Opinion

In our opinion, in all material respects,

a. The description presents Cassidy's system that was designed and implemented for the period April 18, 2026 – July 18, 2026 in accordance with the description criteria.

b. The controls stated in the description were suitably designed for the period April 18, 2026 – July 18, 2026 to provide reasonable assurance that Cassidy's service commitments and system requirements would be achieved based on the applicable HIPAA/HITECH requirements, if its controls operated effectively throughout that period and if the subservice organization applied the

complementary controls assumed in the design of Cassidy controls throughout the period.

c. The controls stated in the description operated effectively throughout the period April 18, 2026 to July 18, 2026, to provide reasonable assurance that Cassidy's service commitments and system requirements were achieved based on the applicable HIPAA/HITECH requirements, if complementary subservice organization controls assumed in the design of Cassidy's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in **Section IV**, is intended solely for the information and use of Cassidy, user entities of the in-scope services for Cassidy Platform systems for the period April 18, 2026 – July 18, 2026, business partners of Cassidy subject to risks arising from interactions with Cassidy Platform system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- Evaluating the overall presentation of the description.
- 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 they interact with related controls at the Service Organization to achieve the Service Organization's 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 HIPAA/HITECH criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

Advantage Partners

September 15, 2026

Section II:
Management's Assertion

Section II: Assertion of Cassidy, Inc. Management

We have prepared the description of Cassidy, Inc. ("Cassidy" or the "Service Organization") health information security program for the Cassidy Platform System (the "Description") for user entities of the system for the period April 18, 2026 – July 18, 2026. We confirm to the best of our knowledge and belief, that:

a) Management's description fairly presents the health information security program for the Cassidy Platform System for the period April 18, 2026 – July 18, 2026. The criteria we used in making this assertion were that the description:

   i) fairly presents how the health information security program was designed and implemented to govern the security policies and practices supporting the Cassidy Platform System
   ii) describes the specified controls within the security program designed to achieve the security program's objectives
   iii) does not omit or distort information relevant to the health information security program for the Cassidy Platform System and may not include every aspect that an individual user entity may consider important in its own particular environment

b) The health information security program governing the Cassidy Platform System complied with applicable requirements of HIPAA and HITECH. The criteria we used in making this assertion were that:

   i) management determined the applicable controls (the "controls") included in the health information security program
   ii) the controls documented complied with the standard and implementation guidance for safeguards as defined by the HIPAA Security Rule including the following:

      - Administrative Safeguards
      - Physical Safeguards
      - Technical Safeguards
      - Organizational Requirements
      - Breach Notification

   iii) the controls stated in the description were suitably designed and implemented for the period April 18, 2026 – July 18, 2026, to provide reasonable assurance that the applicable HIPAA and HITECH requirements would be met, if its controls operated effectively throughout the review period and if the subservice organizations and user entities applied the complementary

controls assumed in the design of Cassidy's controls throughout the review period.

Section III of this report includes Cassidy's description of the health information security program for Cassidy Platform System that is covered by this assertion.

Section III:
Description of the System

Section III: Description of the System

Company Background

Cassidy is an enterprise AI automation platform based in New York City that enables businesses to build sophisticated AI automations without code. The platform combines AI assistants and intelligent workflows to help mid-market and enterprise organizations automate complex business processes while maintaining security and control. Founded in 2023, Cassidy serves organizations across industries including financial services, healthcare, technology, and professional services.

Description of Services Overview

The Cassidy Platform is an enterprise-grade AI automation platform that enables organizations to build intelligent workflows and AI assistants trained on their proprietary data. Built on secure cloud infrastructure, Cassidy provides advanced RAG (Retrieval-Augmented Generation) capabilities, multi-modal AI processing, and seamless integrations with enterprise systems. The platform supports complex automation scenarios including document processing, data analysis, and multi-step business workflows while maintaining data isolation and security.

Cassidy provides comprehensive AI automation capabilities including custom AI assistants with knowledge base integration, intelligent workflow automation with conditional logic and human-in-the-loop processes, and enterprise integrations with 100+ business tools including Salesforce, Microsoft 365, Slack, and proprietary databases. The platform features advanced document processing with OCR and multi-format support, secure data handling with role-based access controls, and real-time collaboration tools. Common use cases include automated RFP and proposal generation, intelligent customer support with ticket routing and response drafting, sales enablement through CRM automation and lead qualification, compliance and audit automation, financial analysis and reporting, and knowledge management across distributed teams.

Principal Service Commitments and System Requirements

Cassidy designs and operates the Cassidy Platform to meet its service commitments and system requirements. These commitments are based on customer agreements, applicable legal and regulatory requirements, and internal security, operational, and compliance requirements.

Cassidy’s commitments to customers are communicated through Master Service Agreements, the Privacy Policy, the Terms of Service, product documentation, and descriptions of the services provided.

Security Commitments

Security commitments include, but are not limited to, the following:

- System features and configuration settings are designed to authorize user access while restricting unauthorized users from accessing information not needed for their role.
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system.
- Regular vulnerability scans over the system and network, and penetration tests over the production environment.
- Operational procedures for managing security incidents and breaches, including notification procedures.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Use of data retention and data disposal.

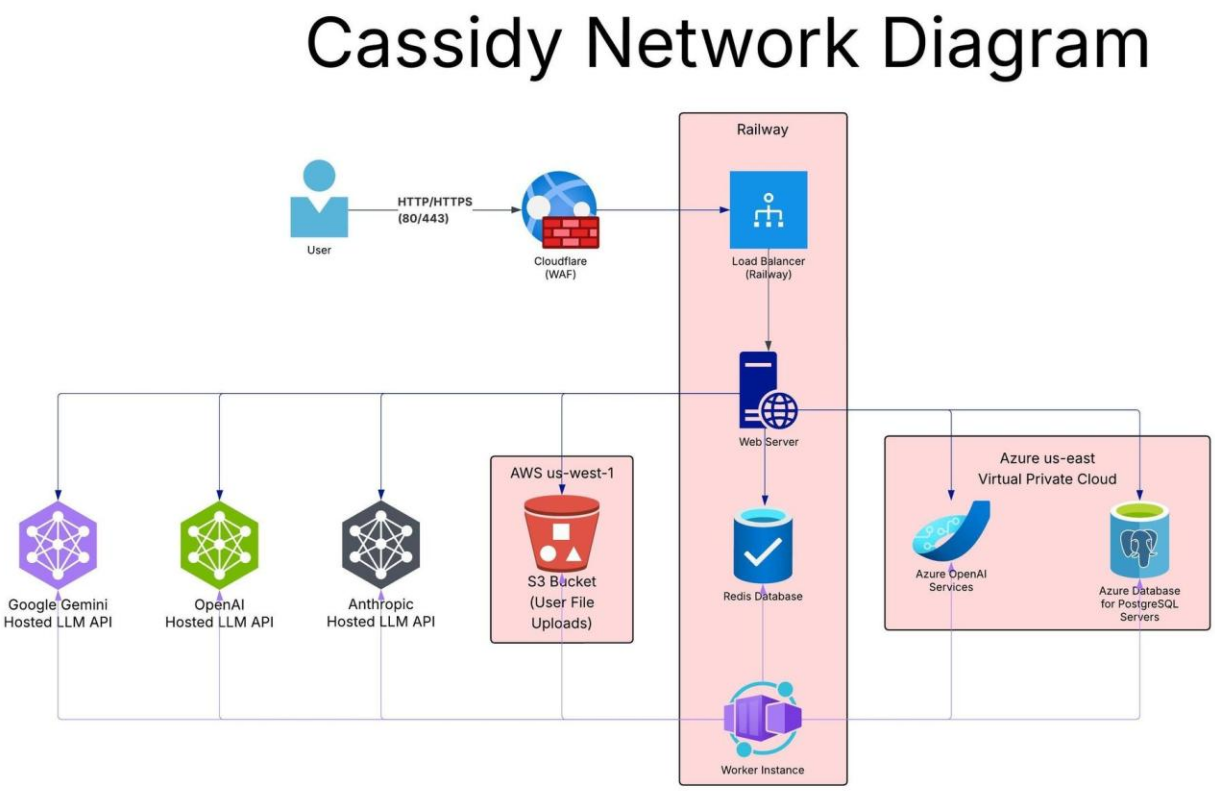
Components of the System

The System description is comprised of the following components:

- Software - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- People - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- Data – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- Procedures – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

Infrastructure

Cassidy maintains inventories of workforce devices, cloud infrastructure, software, and third-party services relevant to the Cassidy Platform. The following diagram presents the principal production services and data flows within the system.



Principal System Components

The following table identifies the material components used to operate, secure, and deliver the Cassidy Platform:

Infrastructure	Type	Purpose
Cassidy Platform	Application	Customer-facing AI automation platform
Railway application and worker services	Application infrastructure	Hosts application services and background processing
Azure Database for PostgreSQL	Data infrastructure	Stores transactional application and customer data
Railway Redis	Data infrastructure	Supports caching and background-job coordination
Amazon S3	Data infrastructure	Stores customer-uploaded files
Cloudflare	Network and security	Routes and protects inbound application traffic
Datadog	Monitoring	Monitors application and infrastructure performance and generates alerts

GitHub	Development and change management	Maintains source code and supports code review and deployment processes
Google Workspace	Workforce identity and administration	Supports workforce identity, email, collaboration, and administration
AI model processing services (Amazon Bedrock, Microsoft Azure OpenAI, OpenAI, Anthropic, and Google Gemini)	External processing	Processes AI requests through the model provider selected for the applicable agent or workflow

The table focuses on components relevant to the scope of this report. It is not intended to represent Cassidy's complete software, asset, vendor, or sub processor inventory.

People

Cassidy employs personnel responsible for management, engineering, product development, operations, information technology, sales, customer support, and marketing. Engineering and Operations personnel monitor the production environment and oversee backup and recovery processes. Personnel receive training appropriate to their responsibilities, including information security requirements.

At the time this description was prepared, Cassidy employed approximately 22 personnel organized across the following functional areas:

Management: Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.

This includes:

- CEO - Justin Fineberg
- CTO - Ian Woodfill

Engineering: Responsible for researching and developing the product, maintaining the security of production infrastructure, testing and deploying the source code of the system.

Product Development: Responsible for the product life cycle, including adding new product functionality. Members of the Product Development team may also be members of the Engineering team.

Operations: Responsible for maintaining the availability of production infrastructure and

managing access and security for production infrastructure. Production access is restricted to authorized Engineering and Operations personnel with a documented business need, subject to least-privilege controls and periodic access reviews. Members of the Operations team may also be members of the Engineering team.

Information Technology: Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.

Sales: Responsible for engaging with prospective customers, managing customer relationships, and supporting the evaluation and onboarding process. Sales personnel do not have access to the production environment or customer data, except as needed to support demos or proof-of-concept implementations.

Customer Support: Responsible for assisting customers with product usage, troubleshooting issues, and relaying feedback to internal teams. Customer Support personnel have access to customer account information as necessary to provide support, but do not have access to production infrastructure.

Marketing: Responsible for brand positioning, communications, demand generation, and customer education. The Marketing team creates and manages content, campaigns, and external messaging, but does not have access to the production environment or sensitive customer data.

Data

Data as defined by Cassidy constitutes the following:

User and account data: User identity, profile, organization, role, access-permission, and usage data for customer personnel and authorized third parties. This data is stored in the transactional database and protected by access controls and encryption at rest.

Customer knowledge base data: Documents, spreadsheets, presentations, text, media, source-code files, and other supported content uploaded or synchronized by customers. Raw files are stored in encrypted Amazon S3 object storage, while processed content, embeddings, and metadata are stored in the platform database to support retrieval and semantic search.

Integration and workflow data: Data synchronized from customer systems through configured integrations and API connections, including CRM records, support tickets, communications, and structured business data. Integration data is encrypted in transit and at rest and logically isolated by customer.

AI processing data: Prompts, retrieved context, conversation histories, workflow execution data, generated content, and assistant interactions. AI requests are routed to the model provider selected for the applicable agent or workflow, which may include Amazon Bedrock, Microsoft Azure OpenAI, OpenAI, Anthropic, or Google Gemini.

Cassidy does not use customer data to train AI models.

Audit and security data: Access logs, permission changes, system events, and other records used for security monitoring, troubleshooting, and compliance. Access to these records is restricted according to job responsibilities.

Data is categorized as the following major types of data used by Cassidy.

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for Cassidy.	• Press releases • Public website
Internal	Access to internal information is approved by management and is protected from external access.	• Internal memos • Design documents • Product specifications • Correspondences
Customer data	Information received from customers for processing or storage by Cassidy. Cassidy must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Customer operating data • Customer PII • Customers' customers' PII • Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by Cassidy to operate the business. Cassidy must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Legal documents • Contractual agreements • Employee PII • Employee salaries

Customer data is managed, processed, retained, and stored in accordance with applicable contractual, legal, and regulatory requirements. Cassidy processes customer data as necessary to provide and support the Cassidy Platform.

All personnel and contractors are required to protect customer data. Cassidy maintains policies and procedures governing the secure handling of customer data, which are reviewed at least annually and updated as needed.

Health Information Security Program Processes, Policies and Procedures

Cassidy has developed a health information security management program to meet the information security and compliance requirements related to Cassidy Platform and its customer base. The program incorporates the elements of the HIPAA and the HITECH. The description below is a summary of safeguards that Cassidy 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 Cassidy 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 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 are 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 Safeguards

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 to 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 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.

Boundaries of the System

The boundaries of this report includes the Health Information Security Program for the Cassidy Platform.

This report does not include the Cloud Hosting Services provided by AWS, Azure and Railway at multiple facilities.

HIPAA/HITECH REQUIREMENTS AND RELATED CONTROLS

Organizational Structure and Assignment of Authority and Responsibility

Cassidy's 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.

Cassidy's 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 they will be held accountable.

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.

HR Policies and Practices

Cassidy's 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 ensure the service organization is operating at maximum efficiency. Cassidy's 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 acknowledgment 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

Cassidy's risk assessment process identifies and manages risks that could potentially affect Cassidy's ability to provide reliable and secure services to our customers. As part of this process, Cassidy maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Cassidy product development process so they can be dealt with predictably and iteratively.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Cassidy's system; as well as the nature of the components of the system result in risks that the criteria will not be met. Cassidy 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, Cassidy's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communication Systems

Information and communication are an integral component of Cassidy's 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.

Cassidy uses several information and communication channels internally to share information with management, employees, contractors, and customers. Cassidy uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, Cassidy uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Cassidy's management performs monitoring activities to continuously 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 are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-going Monitoring

Cassidy's 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.

Management's close involvement in Cassidy's operations helps to identify significant variances in 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 Cassidy's personnel.

Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System

No significant changes have occurred in the system throughout the audit period.

Incidents

No significant incidents have occurred with the services provided to users throughout the audit period.

Requirements Not Applicable to the System

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

HIPAA/HITECH Requirements Not Applicable to the System		
Safeguard	**Requirement**	**Reason**
Administrative Safeguard	164.308(a)(4)(ii)(A)	The entity is not a healthcare clearinghouse.
Physical Safeguard	164.310(c)	The entity is not a covered entity.
	164.314(a)(2)(ii)	The entity is not a government entity.

Organizational Safeguard	164.314(b)(1), 164.314(b)(2)	The entity is not a plan sponsor.
Breach Notification	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 notification are limited to its covered entity customers.

Subservice Organizations

This report does not include the Cloud Hosting Services provided by AWS, Azure and Railway at multiple facilities.

Subservice Description of Services

The Cloud Hosting Services provided by AWS, Azure and Railway support the physical infrastructure of the entity's services.

Complementary Subservice Organization Controls

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

The following subservice organization controls have been implemented by AWS, Azure and Railway and included in this report to provide additional assurance that the applicable HIPAA/HITECH requirements are met.

Subservice Organization - AWS		
Safeguard	**Requirement**	**Control**
Physical Safeguard	164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1)	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Closed circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
		Access to server locations is managed by electronic access control devices.

Subservice Organization - Azure		
Safeguard	**Requirement**	**Control**
Physical Safeguard	164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1)	Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors have been established.
		Security verification and check-in for personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors, are required.
		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.

Subservice Organization - Railway		
Safeguard	**Requirement**	**Control**
Physical Safeguard	164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1)	Physical access to the data center facilities supporting the service is restricted to authorized personnel.

Cassidy management, along with the subservice provider, define the scope and responsibility of the controls necessary to meet all the relevant applicable HIPAA/HITECH requirements through written contracts, such as service level agreements. In addition, Cassidy performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with vendors and subservice organizations.
- Reviewing attestation reports over services provided by vendors and subservice organizations.

Complementary User Entity Controls

Cassidy's 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 applicable HIPAA/HITECH requirements related to Cassidy's services to be solely achieved by Cassidy control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Cassidy's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the applicable 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 performing testing and approvals of the implementation process to ensure that the information is accurate and complete and that the system is functioning as it was requested.
2. User entities are responsible for implementing controls to ensure that inputs are captured accurately, completely and timely.
3. User entities are responsible for implementing controls to ensure that modification of data is authorized.

Section IV: Description of Criteria, Service Auditor Testing

Section IV: Description of Criteria, Service Auditor Testing

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

Part A: HIPAA Safeguards and Service Organization Control Activities

164.308 - Administrative Safeguards

Criteria	Cassidy Control Activity
164.308(a)(1)(i): Security management process: Implement policies and procedures to prevent, detect, contain and correct security violations.	**CA-01** - The company has implemented policies and procedures to prevent, detect, contain, and correct security violations. If the company has committed to an SLA for a security violation, the corrective action is completed within that SLA.
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.	**CA-02** - The company has conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held in its system.
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; and • The probability and criticality of potential risks to ePHI	**CA-03** - The company has implemented security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the HIPAA security general requirements (described in 164.306(a)).
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.	**CA-04** - The company applies appropriate sanctions against workforce members who fail to comply with the security policies and procedures.

164.308 - Administrative Safeguards

Criteria	Cassidy Control Activity
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.	**CA-05** - The company has implemented procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
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.	**CA-06** - The company has implemented policies and procedures to address the final disposition of electronic Protected Health Information (ePHI), and/or the hardware or electronic media on which it is stored. **CA-07** - The company has identified a security official to be responsible for the development and implementation of the policies and procedures required by the HIPAA Security rules for the company.
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	**CA-08** - The company has implemented policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information (ePHI), and to prevent those workforce members who do not have access from obtaining access to ePHI.
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.	**CA-09** - The company has implemented procedures for the authorization and/or supervision of workforce members who work with electronic protected health information (ePHI) or in locations where it might be accessed.
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.	**CA-10** - The company has implemented procedures to determine that the access of a workforce member to electronic protected health information (ePHI) is appropriate.

Criteria	Cassidy Control Activity
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.	**CA-11** - The company has implemented procedures for terminating access to electronic protected health information (ePHI) when the employment of a workforce member ends or as required when access is no longer appropriate.
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.	**CA-12** - The company has implemented policies and procedures for authorizing access to electronic protected health information (ePHI) that are consistent with the applicable privacy rule requirements (subpart E).
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.	**CA-14** - The company has implemented policies and procedures for granting access to electronic protected health information (for example, through access to a workstation, transaction, program, process, or other mechanism).
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.	**CA-15** - The company has implemented policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
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.	**CA-16** - The company has implemented a security awareness and training program for all members of its workforce, including management.

164.308 - Administrative Safeguards

Criteria	Cassidy Control Activity
164.308(a)(5)(ii)(A): Security reminders: Periodic security updates.	**CA-17** - The company conducts periodic security updates.
164.308(a)(5)(ii)(B): Protection from malicious software: Procedures for guarding against, detecting, and reporting malicious software.	**CA-18** - The company has implemented procedures for guarding against, detecting, and reporting malicious software.
164.308(a)(5)(ii)(C): Log-in monitoring: Procedures for monitoring log-in attempts and reporting discrepancies.	**CA-19** - The company has implemented procedures for monitoring log-in attempts and reporting discrepancies.
164.308(a)(5)(ii)(D): Password management: Procedures for creating, changing, and safeguarding passwords.	**CA-20** - The company has implemented procedures for creating, changing, and safeguarding passwords.
164.308(a)(6)(i): Security incident procedures: Implement policies and procedures to address security incidents. Policies and procedures should include response reporting.	**CA-21** - The company has implemented policies and procedures to address security incidents.
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.	**CA-22** - The company identifies and responds to suspected or known security incidents, mitigates, to the extent practicable, harmful effects of security incidents that are known to the company, and documents security incidents and their outcomes.
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.	**CA-23** - The company has established (and implements as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic Protected Health Information (ePHI).
164.308(a)(7)(ii)(A) Data backup plan: Establish and implement procedures to create and maintain retrievable exact copies of ePHI.	**CA-24** - The company has established and implements procedures to create and maintain retrievable exact copies of electronic protected health information (ePHI).
164.308(a)(7)(ii)(B): Disaster recovery plan: Establish (and implement as needed) procedures to restore any loss of data.	**CA-25** - The company has established (and implements as needed) procedures to restore any loss of data.

Criteria	Cassidy Control Activity
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.	**CA-26** - The company has established (and implements as needed) procedures to enable the continuation of critical business processes for the protection and security of electronic Protected Health Information (ePHI) while operating in emergency mode.
164.308(a)(7)(ii)(D): Testing and revision procedures: Implement procedures for periodic testing and revision of contingency plans.	**CA-27** - The company has implemented procedures for periodic testing and revision of contingency plans.
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.	**CA-28** - The company assesses the relative criticality of specific applications and data in support of other contingency plan components.
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.	**CA-29** - The company performs a periodic technical and nontechnical evaluation, based initially upon the HIPAA security rule, and subsequently, in response to environmental or operational changes affecting the security of electronic Protected Health Information (ePHI), establishes the extent to which the company's security policies and procedures meet the requirements of the HIPAA security rule (subpart C).
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.	**CA-30** - The company, as a business associate, permits a business associate to create, receive, maintain, or transmit electronic Protected Health Information (ePHI) on the company's behalf only if it can obtain satisfactory assurances, in accordance with company policies, that the business associate will appropriately safeguard the information.
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.	**CA-31** - The company, as a business associate, may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic Protected Health Information (ePHI) on its behalf only if the company can obtain satisfactory assurances, in accordance with company policies, that the subcontractor will appropriately safeguard the information.

164.308 - Administrative Safeguards

Criteria	Cassidy Control Activity
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]	**CA-16** - The company has implemented a security awareness and training program for all members of its workforce, including management. **CA-30** - The company, as a business associate, permits a business associate to create, receive, maintain, or transmit electronic Protected Health Information (ePHI) on the company's behalf only if it can obtain satisfactory assurances, in accordance with company policies, that the business associate will appropriately safeguard the information. **CA-32 -** The company documents the satisfactory assurances required for business associates and business-associated contractors through a written contract or other arrangements with the business associate that meets the applicable requirements of company policies.

164.310 - Physical Safeguards

Criteria	Cassidy Control Activity
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.	**CA-34** - The company has implemented 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.
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.	**CA-35** - The company has established (and implements 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.
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.	**CA-36** - The company has implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
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.	**CA-37** - The company has implemented 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.
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).	**CA-38** - The company has implemented 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).
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.	**CA-39** - The company has implemented policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic Protected Health Information (ePHI).
164.310(c): Workstation security: Covered entities should implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.	**CA-40** - The company has implemented physical safeguards for all workstations that access electronic protected health information (ePHI), to restrict access to authorized users.

164.310 - Physical Safeguards

Criteria	Cassidy Control Activity
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.	**CA-41** - The company has implemented policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic Protected Health Information (ePHI) into and out of a facility, and the movement of these items within the facility.
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.	**CA-06** - The company has implemented policies and procedures to address the final disposition of electronic Protected Health Information (ePHI), and/or the hardware or electronic media on which it is stored.
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.	**CA-43** - The company has implemented procedures for removal of electronic protected health information (ePHI) from electronic media before the media are made available for re-use.
164.310(d)(2)(iii): Accountability: Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	**CA-44** - The company maintains a record of the movements of hardware and electronic media and any person responsible therefore.
164.310(d)(2)(iv): Data backup and storage: Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.	**CA-45** - The company creates a retrievable, exact copy of electronic protected health information (ePHI), when needed, before the movement of equipment.

164.312 - Technical Safeguards

Criteria	Cassidy Control Activity
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].	**CA-46** - The company implements technical policies and procedures for electronic information systems that maintain electronic protected health information (ePHI) to allow access only to those persons or software programs that have been granted access rights.
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. Ensure that the necessary data is available in the system logs to support audit and other related business functions.	**CA-47** - The company assigns a unique name and/or number for identifying and tracking user identity.
164.312(a)(2)(ii): Emergency access procedure: Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.	**CA-48** - The company has established (and implements as needed) procedures for obtaining necessary electronic protected health information (ePHI) during an emergency.
164.312(a)(2)(iii): Automatic logoff: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	**CA-49** - The company has implemented electronic procedures that terminate an electronic session after a predetermined time of inactivity.
164.312(a)(2)(iv): Encryption and decryption: Implement a mechanism to encrypt and decrypt ePHI.	**CA-50** - The company has implemented a mechanism to encrypt and decrypt electronic protected health information (ePHI).
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.	**CA-51** - The company has implemented hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information (ePHI).
164.312(c)(1): Integrity: Implement policies and procedures to protect ePHI from improper alteration or destruction.	**CA-52** - The company has implemented policies and procedures to protect electronic protected health information (ePHI) from improper alteration or destruction.
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.	**CA-53** - The company has implemented electronic mechanisms to corroborate that electronic protected health information (ePHI) has not been altered or destroyed in an unauthorized manner.

164.312 - Technical Safeguards

Criteria	Cassidy Control Activity
164.312(d): Person or entity authentication: Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	**CA-54** - The company has implemented procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
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.	**CA-55** - The company has implemented technical security measures to guard against unauthorized access to electronic protected health information (ePHI) that is being transmitted over an electronic communications network.
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.	**CA-56** - The company has implemented security measures to ensure that electronically transmitted electronic protected health information (ePHI) is not improperly modified without detection until disposed of.
164.312(e)(2)(ii): Encryption: Implement a mechanism to encrypt ePHI whenever deemed appropriate.	**CA-57** - The company has implemented a mechanism to encrypt electronic protected health information (ePHI) whenever deemed appropriate.

164.314 - Organizational requirements

Criteria	Cassidy Control Activity
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.	**CA-58** - The company requires an agreement contract or other arrangement from business associates that meets administrative safeguards (164.308(b)(3)) and the requirements of the organization (164.314(a)(2)(i), (a)(2)(ii), or (a)(2)(iii)) as applicable.
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."	**CA-59** - The company requires that business associate agreements include compliance with the applicable requirements. **CA-60** - The company requires business associates and subcontractors to report any security incident of which it becomes aware, including breaches of unsecured protected health information as required by the Breach Notification rules (§ 164.410). **CA-61** - The company, in accordance with administrative safeguards (§ 164.308(b)(2)), ensures that any subcontractors that create, receive, maintain, or transmit electronic Protected Health Information (ePHI) on behalf of the business associate agree to comply with the applicable requirements by entering into an agreement contract or other arrangement that complies with organization requirements.
164.314(a)(2)(iii): Business associate contracts with subcontractors: The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by §164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.	**CA-62** - The company requires that the requirements described for 164.314(a)(2)(i) and 164.314(a)(2)(ii) apply to the agreement contract or other arrangements between a business associate and a subcontractor in the same manner as such requirements apply to agreement contracts or other arrangements between the company and the business associate.

164.316 - Policies, procedures and documentation requirements

Criteria	Cassidy Control Activity
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.	**CA-66** - The company, as a business associate, must, in accordance with the HIPAA security rule (§ 164.306), implement reasonable and appropriate policies and procedures to comply with implementation specifications, or other requirements, taking into account those factors specified in the HIPAA security general rules (§ 164.306(b)(2)(i), (ii), (iii), and (iv)). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements (§ 164.316). 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.
164.316(b)(1)(i): 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.	**CA-67** - The company maintains the policies and procedures implemented to comply with the HIPAA security safeguards in written (which may be electronic) form.
164.316(b)(1)(ii): Documentation: 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.	**CA-68** - Where an action, activity or assessment is required (described in 164.316) to be documented, the company maintains a written (which may be electronic) record of the action, activity, or assessment.
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.	**CA-69** - The company retains the documentation of policies, procedures and action, activity or assessments as required by paragraph 316(b)(1) of the HIPAA rules for 6 years from the date of its creation or the date when it last was in effect, whichever is later.
164.316(b)(2)(ii): Availability: Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains	**CA-70** - The company makes documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
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.	**CA-71** - The company reviews documentation periodically, and updates as needed, in response to environmental or operational changes affecting the security of electronic protected health information (ePHI).

164.404 - Notification to individuals

Criteria	Cassidy Control Activity
164.404 (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).	**Not Applicable:** The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers. Refer to the Requirements Applicable to the System in **Section III.**
164.404(a): 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.	**Not Applicable:** The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers. Refer to the Requirements Applicable to the System in **Section III.**
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.	**Not Applicable:** The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers. Refer to the Requirements Applicable to the System in **Section III.**

164.404 - Notification to individuals

Criteria	Cassidy Control Activity
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 investigate 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 email address, website, or postal address.	**Not Applicable:** The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers. Refer to the Requirements Applicable to the System in **Section III.**
164.404(c)(2): The notification required by paragraph (a) of this section shall be written in plain language.	**Not Applicable:** The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers. Refer to the Requirements Applicable to the System in **Section III.**
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.	**Not Applicable:** The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers. Refer to the Requirements Applicable to the System in **Section III.**

164.404 - Notification to individuals

Criteria	Cassidy Control Activity
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.	**Not Applicable:** The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers. Refer to the Requirements Applicable to the System in **Section III.**
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 reasonably 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).	**Not Applicable:** The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers. Refer to the Requirements Applicable to the System in **Section III.**
164.404(d)(2)(i): In the 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.	**Not Applicable:** The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers. Refer to the Requirements Applicable to the System in **Section III.**

164.404 - Notification to individuals

Criteria	Cassidy Control Activity
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) includes 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.	**Not Applicable:** The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers. Refer to the Requirements Applicable to the System in **Section III.**
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.	**Not Applicable:** The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers. Refer to the Requirements Applicable to the System in **Section III.**

164.406 Notification to the media

Criteria	Cassidy Control Activity
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	**Not Applicable:** The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers. Refer to the Requirements Applicable to the System in **Section III.**
164.406(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.	**Not Applicable:** The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers. Refer to the Requirements Applicable to the System in **Section III.**
164.406(c): The content of the notification required by paragraph (a) shall meet the requirements of §164.404(c)	**Not Applicable:** The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers. Refer to the Requirements Applicable to the System in **Section III.**

164.408 Notification to the Secretary

Criteria	Cassidy Control Activity
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.	**CA-72** - A business associate provides the company, as a business associate, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.
164.408(b): For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided, 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.	**Not Applicable:** The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers. Refer to the Requirements Applicable to the System in **Section III.**
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.	**Not Applicable:** The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers. Refer to the Requirements Applicable to the System in **Section III.**

164.410 Notification by a business associate

Criteria	Cassidy Control Activity
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.	**CA-89** - The company, as a business associate, requires all business associates, following the discovery of a breach of unsecured protected health information, to notify the company of such breach. A breach is 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 due diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agents of the business associate (determined in accordance with the Federal common law of agency).
164.410(a)(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).	**CA-89** - The company, as a business associate, requires all business associates, following the discovery of a breach of unsecured protected health information, to notify the company of such breach. A breach is 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 due diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agents of the business associate (determined in accordance with the Federal common law of agency).
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.	**CA-72** - A business associate provides the company, as a business associate, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.
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.	**CA-92 -** A business associate's breach notification includes, 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 disclosed during the breach.

164.410 Notification by a business associate

Criteria	Cassidy Control Activity
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.	**CA-72** - A business associate provides the company, as a business associate, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.

164.502 Uses and disclosures of protected health information: General rules

Criteria	Cassidy Control Activity
164.502(a)(3): Business associates - permitted uses and disclosures: A business associate may use or disclose PHI only as permitted or required by its business associate contract or as required by law, and may not use or disclose PHI in a manner that would violate the Privacy Rule if done by the covered entity.	**CA-95** - The company, acting as a business associate, uses or discloses PHI only as permitted or required by its business associate agreement or as required by law, and makes required disclosures to the Secretary and to the covered entity or individual to support access requests.
164.502(a)(4): Business associates - required uses and disclosures: A business associate is required to disclose PHI when required by the Secretary to investigate its compliance, and to the covered entity, individual, or individual's designee as necessary to satisfy the covered entity's obligations for an individual's request for an electronic copy of PHI.	**CA-95** - The company, acting as a business associate, uses or discloses PHI only as permitted or required by its business associate agreement or as required by law, and makes required disclosures to the Secretary and to the covered entity or individual to support access requests.

164.504 Uses and disclosures: Organizational requirements

Criteria	Cassidy Control Activity
164.504(e)(1): Business associate contracts - standard: The contract or arrangement required by 164.502(e)(2) must meet the applicable requirements; a covered entity (or business associate as to a subcontractor) is not in compliance if it knew of a pattern or practice constituting a material breach and failed to take reasonable steps to cure or terminate.	**CA-96** -The company enters into business associate contracts that establish permitted and required uses and disclosures and obligate the business associate to safeguard PHI, report breaches, flow down terms to subcontractors, support individual rights, make records available to the Secretary, and return or destroy PHI at termination.
164.504(e)(2): Business associate contract content: The contract must establish permitted and required uses/disclosures and obligate the business associate to not use or disclose PHI improperly, use appropriate safeguards, report improper uses/disclosures and breaches, bind subcontractors to the same conditions, support individual access/amendment/accounting, make records available to the Secretary, and return or destroy PHI at termination.	**CA-96** - The company enters into business associate contracts that establish permitted and required uses and disclosures and obligate the business associate to safeguard PHI, report breaches, flow down terms to subcontractors, support individual rights, make records available to the Secretary, and return or destroy PHI at termination.
164.504(e)(4): Other requirements for contracts and arrangements: The contract may permit the business associate to use or disclose PHI for its own proper management and administration or legal responsibilities, if required by law or made with reasonable assurances of confidentiality and breach notification from the recipient.	**CA-97** - The company, acting as a business associate, uses or discloses PHI for its own proper management and administration or legal responsibilities only as the contract permits and with required confidentiality and breach-notice assurances.
164.504(e)(5): Business associate contracts with subcontractors: The requirements of 164.504(e)(2)-(e)(4) apply to the contract between a business associate and a subcontractor in the same manner as between a covered entity and business associate.	**CA-98** - The company, acting as a business associate, requires subcontractors that handle PHI on its behalf to enter into contracts subject to the same restrictions and conditions that apply to the company.

Part B: Testing of Controls and Results

Control Activity	Tests Performed	Test Results
CA-01 - The company has implemented policies and procedures to prevent, detect, contain, and correct security violations. If the company has committed to an SLA for a security violation, the corrective action is completed within that SLA.	Inspected the signed Incident Response Policy for a sample of employees to determine employees agreed to the policy. Inspected the Incident Response Policy to determine that the company had security and privacy incident response policies in place. Inspected the Information Security Policy for a sample of employees to determine employees agreed to the policy. Inspected the Operation Security Policy to determine that host-based vulnerability scans were performed at least quarterly on all external-facing systems, and that critical and high vulnerabilities were tracked to remediation.	No exceptions noted.
CA-02 - The company has conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held in its system.	Inspected the Completed HIPAA risk review to determine that the company had conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held in its system. Inspected the Risk Management Policy to determine that the company had a documented risk management program in place, including guidance on the identification of potential threats, rating the significance of risks associated with identified threats, and mitigation strategies for those risks.	No exceptions noted.
CA-03 - The company has implemented security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the HIPAA security general requirements (described in § 164.306(a)).	Inspected the Completed HIPAA risk review to determine that the company had conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held in its system. Inspected the Risk Management Policy to determine that the company had a documented risk management program in place, including guidance on the identification of potential threats, rating the significance of risks associated with identified threats, and mitigation strategies for those risks. Inspected the completed background check to determine that the company required background checks on new employees.	No exceptions noted.
CA-04 - The company applies appropriate sanctions against workforce members who fail to comply with the security policies and procedures.	Inspected the Information Security Policy for a sample of employees to determine employees agreed to the policy. Inspected the HIPAA Compliance Policy to determine that the company had a policy in place to comply with HIPAA requirements.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-05 - The company has implemented procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Inspected the Incident Response Policy to determine that the company had security and privacy incident response policies in place. Inspected the Operation Security Policy to determine that host-based vulnerability scans were performed at least quarterly on all external-facing systems, and that critical and high vulnerabilities were tracked to remediation. Inspected the resolved security incidents to determine that the company assigned security issues to relevant owners. Inspected the access policies of the company to determine that the company's access control policy documented the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access.	Testing of this control activity disclosed that there were no security incidents noted during the review period.
CA-06 - The company has implemented policies and procedures to address the final disposition of electronic Protected Health Information (ePHI), and/or the hardware or electronic media on which it is stored.	Inspected the Asset Management Policy to determine that the company had implemented policies and procedures to address the final disposition of electronic Protected Health Information (ePHI), and/or the hardware or electronic media on which it was stored Inspected the Data Management Policy to determine that the company had implemented policies and procedures to address the final disposition of electronic Protected Health Information (ePHI), and/or the hardware or electronic media on which it was stored	No exceptions noted.
CA-07 - The company has identified a security official to be responsible for the development and implementation of the policies and procedures required by the HIPAA Security rules for the company.	Inspected the HIPAA Compliance Policy to determine that the company had a policy in place to comply with HIPAA requirements.	No exceptions noted.
CA-08 - The company has implemented policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information (ePHI), and to prevent those workforce members who do not have access from obtaining access to ePHI.	Inspected the access policies of the company to determine that the company's access control policy documented the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. Inspected the company's user listings to determine that the company restricts privileged access to encryption keys to authorized users with a business need.	No exceptions noted.
CA-09 - The company has implemented procedures for the authorization and/or supervision of workforce members who work with electronic protected health information (ePHI) or in locations where it might be accessed.	Inspected the access policies of the company to determine that the company's access control policy documented the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. Inspected the company's user listings to determine that the company restricts privileged access to encryption keys to authorized users with a business need.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-10 - The company has implemented procedures to determine that the access of a workforce member to electronic protected health information (ePHI) is appropriate.	Inspected the access policies of the company to determine that the company's access control policy documented the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. Inspected the company's user listings to determine that the company restricts privileged access to encryption keys to authorized users with a business need.	No exceptions noted.
CA-11 - The company has implemented procedures for terminating access to electronic protected health information (ePHI) when the employment of a workforce member ends or as required when access is no longer appropriate.	Inspected the access policies of the company to determine that the company's access control policy documented the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. Inspected the company user listings and a sample of terminated users to determine that the company completed termination checklists for terminated employees and was within defined SLAs.	No exceptions noted.
CA-12 - The company has implemented policies and procedures for authorizing access to electronic protected health information (ePHI) that are consistent with the applicable privacy rule requirements (subpart E).	Inspected the access policies of the company to determine that the company's access control policy documented the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access.	No exceptions noted.
CA-14 - The company has implemented policies and procedures for granting access to electronic protected health information (for example, through access to a workstation, transaction, program, process, or other mechanism).	Inspected the access policies of the company to determine that the company's access control policy documented the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. Inspected the company's user listings to determine that the company restricts privileged access to encryption keys to authorized users with a business need.	No exceptions noted.
CA-15 - The company has implemented policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Inspected the access policies of the company to determine that the company's access control policy documented the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. Inspected the company's user listings for in-scope system components to ensure all accounts are associated with users.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-16 - The company has implemented a security awareness and training program for all members of its workforce, including management.	Inspected the information security program to determine that the company had implemented a security awareness and training program for all members of its workforce, including management.. Inspected the information security training program to determine that the company required current employees to complete security awareness training at least annually. Inspected the completed information security training to determine that the company required current employees to complete security awareness training at least annually. Inspected the Human Resource Policy to determine that the company had implemented a security awareness and training program for all members of its workforce, including management..	No exceptions noted.
CA-18 - The company has implemented procedures for guarding against, detecting, and reporting malicious software.	Inspected the Operation Security Policy to determine that host-based vulnerability scans were performed at least quarterly on all external-facing systems, and that critical and high vulnerabilities were tracked to remediation. Inspected the MDM tool dashboard for a sample of endpoint devices to determine that the company deployed anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems. Inspected the company's MDM tool configurations to determine that the company provides continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
CA-19 - The company has implemented procedures for monitoring log-in attempts and reporting discrepancies.	Inspected the CloudTrail configurations to determine that the company utilized a log management tool to identify and track events that may have potential impact on the company's ability to achieve its security objectives.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-20 - The company has implemented procedures for creating, changing, and safeguarding passwords.	Inspected the Information Security Policy for a sample of employees to determine employees agreed to the policy. Inspected the access policies of the company to determine that the company's access control policy documented the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. Observed that password managers were in use on user endpoints to determine that the company required passwords for in-scope system components to be configured according to the company's policy. Inspected the access policies of the company to determine that the company had implemented procedures for creating, changing, and safeguarding passwords. Inspected the company's MDM tool configurations to determine that the company had a password manager installed on employee end points supporting the service.	No exceptions noted.
CA-21 - The company has implemented policies and procedures to address security incidents.	Inspected the Incident Response Policy to determine that the company had security and privacy incident response policies in place. Inspected the Information Security Policy for a sample of employees to determine employees agreed to the policy. Inspected the resolved security incidents to determine that the company assigned security issues to relevant owners. Inspected the resolved security incidents for a sample of security incidents to determine that the company required security and privacy incidents to be logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. Inspected a sample of remediated vulnerabilities to determine that the company had infrastructure supporting the service patching as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats.	Testing of this control activity disclosed that there were no security incidents noted during the review period.
CA-22 - The company identifies and responds to suspected or known security incidents, mitigates, to the extent practicable, harmful effects of security incidents that are known to the company, and documents security incidents and their outcomes.	Inspected the Incident Response Policy to determine that the company had security and privacy incident response policies in place. Inspected the Information Security Policy for a sample of employees to determine employees agreed to the policy. Inspected the resolved security incidents to determine that the company assigned security issues to relevant owners.	Testing of this control activity disclosed that there were no security incidents noted during the review period.

Control Activity	Tests Performed	Test Results
CA-23 - The company has established (and implements as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic Protected Health Information (ePHI).	Inspected the Business Continuity and Disaster Recovery Policy to determine that the company established (and implements as needed) policies and procedures for responding to an emergency or other occurrence that damages systems that contain ePHI.	No exceptions noted.
CA-24 - The company has established and implemented procedures to create and maintain retrievable exact copies of electronic protected health information (ePHI).	Inspected the Operation Security Policy to determine that the company established and implemented procedures to create and maintain retrievable exact copies of electronic protected health information (ePHI). Inspected the configuration of the company's cloud environment to determine that the company established and implemented procedures to create and maintain retrievable exact copies of electronic protected health information (ePHI).	No exceptions noted.
CA-25 - The company has established (and implements as needed) procedures to restore any loss of data.	Inspected the Operation Security Policy to determine that the company established (and implemented as needed) procedures to restore any loss of data. Inspected the Business Continuity and Disaster Recovery Policy to determine that the company established (and implemented as needed) procedures to restore any loss of data.	No exceptions noted.
CA-26 - The company has established (and implements as needed) procedures to enable the continuation of critical business processes for the protection and security of electronic Protected Health Information (ePHI) while operating in emergency mode.	Inspected the Business Continuity and Disaster Recovery Policy to determine that the company established (and implemented as needed) procedures to enable the continuation of critical business processes for the protection and security of ePHI while operating in emergency mode.	No exceptions noted.
CA-27 - The company has implemented procedures for periodic testing and revision of contingency plans.	Inspected the Business Continuity and Disaster Recovery Policy to determine that the company implemented procedures for periodic testing and revision of contingency plans	No exceptions noted.
CA-28 - The company assesses the relative criticality of specific applications and data in support of other contingency plan components.	Inspected the Completed HIPAA risk review to determine that the company had a documented risk management program in place, including guidance on the identification of potential threats, rating the significance of risks associated with identified threats, and mitigation strategies for those risks. Inspected the Risk Management Policy to determine that the company had a documented risk management program in place, including guidance on the identification of potential threats, rating the significance of risks associated with identified threats, and mitigation strategies for those risks.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-29 - The company performs a periodic technical and nontechnical evaluation, based initially upon the HIPAA security rule, and subsequently, in response to environmental or operational changes affecting the security of electronic Protected Health Information (ePHI), establishes the extent to which the company's security policies and procedures meet the requirements of the HIPAA security rule (subpart C).	Inspected the Risk Management Policy to determine that the company had a documented risk management program in place, including guidance on the identification of potential threats, rating the significance of risks associated with identified threats, and mitigation strategies for those risks. Inspected a sample of remediated vulnerabilities to determine that the company had infrastructure supporting the service patching as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats. Inspected the vulnerability scanning configurations to determine that host-based vulnerability scans were performed at least quarterly on all external-facing systems, and that critical and high vulnerabilities were tracked to remediation. Inspected the remediated vulnerability tickets for a sample of vulnerabilities found in critical systems to determine that host-based vulnerability scans were performed at least quarterly on all external-facing systems, and that critical and high vulnerabilities were tracked to remediation.	No exceptions noted.
CA-30 - The company, as a business associate, permits a business associate to create, receive, maintain, or transmit electronic Protected Health Information (ePHI) on the company's behalf only if it can obtain satisfactory assurances, in accordance with company policies, that the business associate will appropriately safeguard the information.	Inspected the HIPAA Compliance Policy to determine that the company had a policy in place to comply with HIPAA requirements. Inspected the list of vendors to determine that the company had written agreements in place with vendors and related third-parties. These agreements included confidentiality and privacy commitments applicable to that entity. Inspected a sample of third-party vendors to determine the company assigned risks to vendors. Inspected the company’s user listings for in-scope system components to ensure all accounts are associated with users. Inspected the Signed HIPAA Compliance Policy to determine that the company permitted a business associate to create, receive, maintain, or transmit ePHI on the company's behalf only if it can obtain satisfactory assurances that the business associate will appropriately safeguard the information.	No exceptions noted.
CA-31 - The company, as a business associate, may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic Protected Health Information (ePHI) on its behalf only if the company can obtain satisfactory assurances, in accordance with company policies, that the subcontractor will appropriately safeguard the information.	Inspected the HIPAA Compliance Policy to determine that the company had a policy in place to comply with HIPAA requirements. Inspected the company’s user listings for in-scope system components to ensure all accounts are associated with users.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-34 - The company has implemented 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.	Inspected the company's user listings for in-scope system components to ensure all accounts are associated with users. Inspected the Third Party Management Policy to determine that the company implemented 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. Inspected the Physical Security Policy to determine that the company has processes in place for granting, changing, and terminating physical access to company data centers based on an authorization from control owners.	No exceptions noted.
CA-35 - The company has established (and implements 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.	Inspected the Business Continuity and Disaster Recovery Policy to determine that the company established (and implements 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 Inspected the Signed Business Continuity and Disaster Recovery Policy to determine that the company established (and implements 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	No exceptions noted.
CA-36 - The company has implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	Inspected the company's user listings for in-scope system components to ensure all accounts are associated with users. Inspected the Third Party Management Policy to determine that the company implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. Inspected the Physical Security Policy to determine that the company has processes in place for granting, changing, and terminating physical access to company data centers based on an authorization from control owners.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-37 - The company has implemented 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.	Inspected the company's user listings for in-scope system components to ensure all accounts are associated with users. Inspected the Third Party Management Policy to determine that the company implemented 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.. Inspected the Physical Security Policy to determine that the company has processes in place for granting, changing, and terminating physical access to company data centers based on an authorization from control owners. Inspected the attestation report and security assessments to determine that the company implemented 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..	No exceptions noted.
CA-38 - The company has implemented 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).	Inspected the Physical Security Policy to determine that the company has processes in place for granting, changing, and terminating physical access to company data centers based on an authorization from control owners.	No exceptions noted.
CA-39 - The company has implemented policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic Protected Health Information (ePHI).	Inspected the HIPAA Workstation Security Policy to determine that the company implemented policies and procedures that specify the proper functions to be performed and the physical attributes of the surroundings of a specific workstation that can access ePHI. Inspected the Asset Management Policy to determine that the company restricted privileged access to the firewall to authorized users with a business need.	No exceptions noted.
CA-40 - The company has implemented physical safeguards for all workstations that access electronic protected health information (ePHI), to restrict access to authorized users.	Inspected the HIPAA Workstation Security Policy to determine that the company had implemented physical safeguards for all workstations that access electronic protected health information (ePHI), to restrict access to authorized users. Inspected the Signed HIPAA Workstation Security Policy to determine that the company had implemented physical safeguards for all workstations that access electronic protected health information (ePHI), to restrict access to authorized users.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-41 - The company has implemented policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic Protected Health Information (ePHI) into and out of a facility, and the movement of these items within the facility.	Inspected the Asset Management Policy to determine that the company 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.	No exceptions noted.
CA-43 - The company has implemented procedures for removal of electronic protected health information (ePHI) from electronic media before the media are made available for re-use.	Inspected the HIPAA Compliance Policy to determine that the company had implemented procedures for removal of electronic protected health information (ePHI) from electronic media before the media was made available for re-use. Inspected the Signed HIPAA Compliance Policy to determine that the company had implemented procedures for removal of electronic protected health information (ePHI) from electronic media before the media was made available for re-use. Inspected the Asset Management Policy to determine that the company had implemented procedures for removal of electronic protected health information (ePHI) from electronic media before the media was made available for re-use. Inspected the Data Management Policy to determine that the company had implemented procedures for removal of electronic protected health information (ePHI) from electronic media before the media was made available for re-use.	No exceptions noted.
CA-44 - The company maintains a record of the movements of hardware and electronic media and any person responsible therefore.	Inspected the Asset Management Policy to determine that the company maintained a record of the movements of hardware and electronic media and any person responsible. Inspected the Data Management Policy to determine that the company maintained a record of the movements of hardware and electronic media and any person responsible.	No exceptions noted.
CA-45 - The company creates a retrievable, exact copy of electronic protected health information (ePHI), when needed, before the movement of equipment.	Inspected the HIPAA Compliance Policy to determine that the company had created a retrievable, exact copy of electronic protected health information (ePHI), when needed, before the movement of equipment. Inspected the company's AWS account to determine that the company had created a retrievable, exact copy of electronic protected health information (ePHI), when needed, before the movement of equipment.	No exceptions noted.
CA-46 - The company implements technical policies and procedures for electronic information systems that maintain electronic protected health information (ePHI) to allow access only to those persons or software programs that have been granted access rights.	Inspected the access policies of the company to determine that the company's access control policy documented the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. Inspected the company's user listings to determine that the company restricts privileged access to encryption keys to authorized users with a business need.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-47 - The company assigns a unique name and/or number for identifying and tracking user identity.	Inspected the access policies of the company to determine that the company's access control policy documented the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. Inspected the administrator user listings to critical applications to determine that the company restricted privileged access to the application to authorized users with a business need.	No exceptions noted.
CA-48 - The company has established (and implements as needed) procedures for obtaining necessary electronic protected health information (ePHI) during an emergency.	Inspected the Business Continuity and Disaster Recovery Policy to determine that the company established (and implemented as needed) procedures for obtaining necessary electronic protected health information (ePHI) during an emergency.	No exceptions noted.
CA-49 - The company has implemented electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Inspected the access policies of the company to determine that the company's access control policy documented the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. Inspected the access policies to determine that the company established (and implemented as needed) procedures for obtaining necessary electronic protected health information (ePHI) during an emergency. Inspected the screen lock configuration to determine that the company established (and implemented as needed) procedures for obtaining necessary electronic protected health information (ePHI) during an emergency.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-50 - The company has implemented a mechanism to encrypt and decrypt electronic protected health information (ePHI).	Inspected the Cryptography Policy to determine that the company had implemented a mechanism to encrypt and decrypt electronic protected health information (ePHI).. Inspected the company's AWS account to determine that the company had implemented a mechanism to encrypt and decrypt electronic protected health information (ePHI). Inspected the load balancer configurations to determine that the company had implemented a mechanism to encrypt and decrypt electronic protected health information (ePHI).. Inspected the encryption configurations to determine that the company had implemented a mechanism to encrypt and decrypt electronic protected health information (ePHI).. Inspected the SSL configurations to determine that the company had implemented a mechanism to encrypt and decrypt electronic protected health information (ePHI).. Inspected the SSL certificate to determine that the company had implemented a mechanism to encrypt and decrypt electronic protected health information (ePHI).. Inspected the AWS account encryption configurations to determine that the company had implemented a mechanism to encrypt and decrypt electronic protected health information (ePHI)..	No exceptions noted.
CA-51 - The company has implemented hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information (ePHI).	Inspected the CloudTrail configurations to determine that the company utilized a log management tool to identify and track events that may have potential impact on the company's ability to achieve its security objectives.	No exceptions noted.
CA-52 - The company has implemented policies and procedures to protect electronic protected health information (ePHI) from improper alteration or destruction.	Inspected the Information Security Policy for a sample of employees to determine employees agreed to the policy. Inspected the HIPAA Compliance Policy to determine that the company had a policy in place to comply with HIPAA requirements. Inspected the access policies of the company to determine that the company's access control policy documented the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-53 - The company has implemented electronic mechanisms to corroborate that electronic protected health information (ePHI) has not been altered or destroyed in an unauthorized manner.	Inspected the CloudTrail configurations to determine that the company utilized a log management tool to identify and track events that may have potential impact on the company's ability to achieve its security objectives. Inspected the vulnerability scanning configurations to determine that host-based vulnerability scans were performed at least quarterly on all external-facing systems, and that critical and high vulnerabilities were tracked to remediation. Inspected the remediated vulnerability tickets for a sample of vulnerabilities found in critical systems to determine that host-based vulnerability scans were performed at least quarterly on all external-facing systems, and that critical and high vulnerabilities were tracked to remediation.	No exceptions noted.
CA-54 - The company has implemented procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Inspected the access policies of the company to determine that the company's access control policy documented the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. Inspected the database user listing and password configurations to determine that the company required authentication to production datastores to use authorized secure authentication mechanisms. Inspected the access policies of the company to determine that the company implemented procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Inspected the company's user listings, system and password configurations to determine that the company's production systems can only be remotely accessed by authorized employees possessing a valid MFA method. Inspected the administrator user listings to critical applications to determine that the company restricted privileged access to the application to authorized users with a business need.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-55 - The company has implemented technical security measures to guard against unauthorized access to electronic protected health information (ePHI) that is being transmitted over an electronic communications network.	Inspected the company's data management policies to determine that the company had formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. Inspected the company's cloud load balancer configurations to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. Inspected the SSL certificates to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. Inspected the database user listing and password configurations to determine that the company required authentication to production datastores to use authorized secure authentication mechanisms. Inspected the EC2 port configurations to determine that the company port configurations restricted privileged access to the firewall to authorized users with a business need. Inspected the company's AWS account to determine that the company port configurations restricted privileged access to the firewall to authorized users with a business need. Inspected the company's data management policies to determine that the company implemented technical security measures to guard against unauthorized access to electronic protected health information (ePHI) that is being transmitted over an electronic communications network. Inspected the company's user listings, system and password configurations to determine that the company's production systems can only be remotely accessed by authorized employees possessing a valid MFA method.	No exceptions noted.
CA-56 - The company has implemented security measures to ensure that electronically transmitted electronic protected health information (ePHI) is not improperly modified without detection until disposed of.	Inspected the company's data management policies to determine that the company had formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. Inspected the Cryptography Policy to determine that the company's datastores housing sensitive customer data were encrypted at rest. Inspected the SSL certificates to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. Inspected the AWS log configurations to determine that the company utilized a log management tool to identify and track events that may have potential impact on the company's ability to achieve its security objectives.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-57 - The company has implemented a mechanism to encrypt electronic protected health information (ePHI) whenever deemed appropriate.	Inspected the Data Management Policy to determine that the company' has implemented a mechanism to encrypt electronic protected health information (ePHI) whenever deemed appropriate. Inspected the Cryptography Policy to determine that the company' has implemented a mechanism to encrypt electronic protected health information (ePHI) whenever deemed appropriate. Inspected the AWS log configurations to determine that the company' has implemented a mechanism to encrypt electronic protected health information (ePHI) whenever deemed appropriate.	No exceptions noted.
CA-58 - The company requires an agreement contract or other arrangement from business associates that meets administrative safeguards (§ 164.308(b)(3)) and the requirements of the organization (§ 164.314(a)(2)(I), (a)(2)(ii), or (a)(2)(iii)) as applicable.	Inspected the HIPAA Compliance Policy to determine that the company had a policy in place to comply with HIPAA requirements. Inspected the company's user listings for in-scope system components to ensure all accounts are associated with users.	No exceptions noted.
CA-59 - The company requires that business associate agreements include compliance with the applicable requirements.	Inspected the HIPAA Compliance Policy to determine that the company had a policy in place to comply with HIPAA requirements. Inspected the company's user listings for in-scope system components to ensure all accounts are associated with users.	No exceptions noted.
CA-61 - The company, in accordance with administrative safeguards (§ 164.308(b)(2)), ensures that any subcontractors that create, receive, maintain, or transmit electronic Protected Health Information (ePHI) on behalf of the business associate agree to comply with the applicable requirements by entering into an agreement contract or other arrangement that complies with organization requirements.	Inspected the company's user listings for in-scope system components to ensure all accounts are associated with users. Inspected the Signed HIPAA Compliance Policy to determine that the company implemented 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 customers.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-62 - The company requires that the requirements described for § 164.314(a)(2)(I) and § 164.314(a)(2)(ii) apply to the agreement contract or other arrangements between a business associate and a subcontractor in the same manner as such requirements apply to agreement contracts or other arrangements between the company and the business associate.	Inspected the HIPAA Compliance Policy to determine that the company had a policy in place to comply with HIPAA requirements. Inspected the company's user listings for in-scope system components to ensure all accounts are associated with users. Inspected the Signed HIPAA Compliance Policy to determine that the company implemented 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 customers.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-63 - The company has implemented administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information (ePHI) that it creates, receives, maintains, or transmits on behalf of the customers.	Inspected the Incident Response Policy to determine that the company had security and privacy incident response policies in place. Inspected the Information Security Policy for a sample of employees to determine employees agreed to the policy. Inspected the Risk Management Policy to determine that the company had a documented risk management program in place, including guidance on the identification of potential threats, rating the significance of risks associated with identified threats, and mitigation strategies for those risks. Inspected the access policies of the company to determine that the company's access control policy documented the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. Inspected the Human Resource Policy to determine that the company implemented 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 customers. Inspected the Business Continuity and Disaster Recovery Policy to determine that the company implemented 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 customers. Inspected the Asset Management Policy to determine that the company restricted privileged access to the firewall to authorized users with a business need. Inspected the company's data management policies to determine that the company had formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. Inspected the Cryptography Policy to determine that the company's datastores housing sensitive customer data were encrypted at rest. Inspected the Information Security Role and Responsibilities Policy to determine that the company implemented 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 customers.	No exceptions noted.
CA-65 - The company reports to the customers any security incident of which it becomes aware.	Inspected the Incident Response Policy to determine that the company had security and privacy incident response policies in place.	No exceptions noted.

CA-66 - The company, as a business associate, must, in accordance with the HIPAA security rule (§ 164.306), implement reasonable and appropriate policies and procedures to comply with implementation specifications, or other requirements, taking into account those factors specified in the HIPAA security general rules (§ 164.306(b)(2)(I), (ii), (iii), and (iv)). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements (§164.316). 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.	Inspected the Risk Management Policy to determine that the company had a documented risk management program in place, including guidance on the identification of potential threats, rating the significance of risks associated with identified threats, and mitigation strategies for those risks. Inspected the access policies of the company to determine that the company's access control policy documented the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. Inspected the Human Resource Policy to determine that the company maintained the policies and procedures implemented to comply with the HIPAA security safeguards in written (which may be electronic) form. Inspected the Business Continuity and Disaster Recovery Policy to determine that the company maintained the policies and procedures implemented to comply with the HIPAA security safeguards in written (which may be electronic) form. Inspected the Asset Management Policy to determine that the company restricted privileged access to the firewall to authorized users with a business need. Inspected the company's Data management policies to determine that the company had formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. Inspected the Cryptography Policy to determine that the company's datastores housing sensitive customer data were encrypted at rest. Inspected the Information Security Policy to determine that the company, as a business associate, must, in accordance with the HIPAA security rule (§ 164.306), implement reasonable and appropriate policies and procedures to comply with implementation specifications, or other requirements, taking into account those factors specified in the HIPAA security general rules (§ 164.306(b)(2)(i), (ii), (iii), and (iv)), Inspected the Physical Security Policy to determine that the company, as a business associate, must, in accordance with the HIPAA security rule (§ 164.306), implement reasonable and appropriate policies and procedures to comply with implementation specifications, or other requirements, taking into account those factors specified in the HIPAA security general rules (§ 164.306(b)(2)(i), (ii), (iii), and (iv)), Inspected the Operations Security Policy to determine that the company, as a business associate, must, in accordance with the HIPAA security rule (§ 164.306), implement reasonable and appropriate policies and procedures to comply with implementation specifications, or other requirements, taking into account those factors specified in the HIPAA security general rules (§ 164.306(b)(2)(i), (ii), (iii), and (iv)), Inspected the Secure Development Policy to determine that the company, as a business associate, must, in accordance with the HIPAA security rule (§ 164.306), implement	No exceptions noted.

Control Activity	Tests Performed	Test Results
	reasonable and appropriate policies and procedures to comply with implementation specifications, or other requirements, taking into account those factors specified in the HIPAA security general rules (§ 164.306(b)(2)(i), (ii), (iii), and (iv)), Inspected the Third-Party Management Policy to determine that the company, as a business associate, must, in accordance with the HIPAA security rule (§ 164.306), implement reasonable and appropriate policies and procedures to comply with implementation specifications, or other requirements, taking into account those factors specified in the HIPAA security general rules (§ 164.306(b)(2)(i), (ii), (iii), and (iv)), Inspected the Incident Response Policy to determine that the company, as a business associate, must, in accordance with the HIPAA security rule (§ 164.306), implement reasonable and appropriate policies and procedures to comply with implementation specifications, or other requirements, taking into account those factors specified in the HIPAA security general rules (§ 164.306(b)(2)(i), (ii), (iii), and (iv)), Inspected the HIPAA Compliance Policy to determine that the company, as a business associate, must, in accordance with the HIPAA security rule (§ 164.306), implement reasonable and appropriate policies and procedures to comply with implementation specifications, or other requirements, taking into account those factors specified in the HIPAA security general rules (§ 164.306(b)(2)(i), (ii), (iii), and (iv)), Inspected the Information Security Roles and Responsibilities Policy to determine that the company, as a business associate, must, in accordance with the HIPAA security rule (§ 164.306), implement reasonable and appropriate policies and procedures to comply with implementation specifications, or other requirements, taking into account those factors specified in the HIPAA security general rules (§ 164.306(b)(2)(i), (ii), (iii), and (iv)),	

CA-67 - The company maintains the policies and procedures implemented to comply with the HIPAA security safeguards in written (which may be electronic) form.	Inspected the Risk Management Policy to determine that the company had a documented risk management program in place, including guidance on the identification of potential threats, rating the significance of risks associated with identified threats, and mitigation strategies for those risks. Inspected the access policies of the company to determine that the company's access control policy documented the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. Inspected the Human Resource Policy to determine that the company maintained the policies and procedures implemented to comply with the HIPAA security safeguards in written (which may be electronic) form. Inspected the relevant information security policies to determine that the company's information security policies and procedures were documented and reviewed at least annually. Inspected the Asset Management Policy to determine that the company restricted privileged access to the firewall to authorized users with a business need. Inspected the company's data management policies to determine that the company had formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. Inspected the Cryptography Policy to determine that the company's datastores housing sensitive customer data were encrypted at rest. Inspected the Information Security Policy (AUP) to determine that the company maintains the policies and procedures implemented to comply with the HIPAA security safeguards in written (which may be electronic) form Inspected the Physical Security Policy to determine that the company maintains the policies and procedures implemented to comply with the HIPAA security safeguards in written (may be electronic) form Inspected the Operations Security Policy to determine that the company maintains the policies and procedures implemented to comply with the HIPAA security safeguards in written (which may be electronic) form Inspected the Secure Development Policy to determine that the company maintains the policies and procedures implemented to comply with the HIPAA security safeguards in written (which may be electronic) form Inspected the Third-Party Management Policy to determine that the company maintains the policies and procedures implemented to comply with the HIPAA security safeguards in written (which may be electronic) form Inspected the Incident Response Policy to determine that the company maintains the policies and procedures implemented	No exceptions noted.

Control Activity	Tests Performed	Test Results
	to comply with the HIPAA security safeguards in written (which may be electronic) form Inspected the HIPAA Compliance Policy to determine that the company maintains the policies and procedures implemented to comply with the HIPAA security safeguards in written (which may be electronic) form Inspected the Information Security roles and responsibilities to determine that the company maintains the policies and procedures implemented to comply with the HIPAA security safeguards in written (which may be electronic) form	
CA-68 - Where an action, activity or assessment is required (described in § 164.316) to be documented, the company maintains a written (which may be electronic) record of the action, activity, or assessment.	Inspected the Information Security Policy for a sample of employees to determine employees agreed to the policy. Inspected the Completed HIPAA risk review to determine that the company had conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held in its system. Inspected the HIPAA Compliance Policy to determine that the company had a policy in place to comply with HIPAA requirements. Inspected the access policies of the company to determine that the company's access control policy documented the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. Inspected the company's data management policies to determine that the company had formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	No exceptions noted.
CA-69 - The company retains the documentation of policies, procedures and action, activity or assessments as required by paragraph 316(b)(1) of the HIPAA rules for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	Inspected the HIPAA Compliance Policy to determine that the company had a policy in place to comply with HIPAA requirements.	No exceptions noted.
CA-70 - The company makes documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Inspected the Information Security Role and Responsibilities Policy to determine that employees agreed to the policies. Inspected the signed company policies for a sample of employees to determine that employees agreed to the policies.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-71 - The company reviews documentation periodically, and updates as needed, in response to environmental or operational changes affecting the security of electronic protected health information (ePHI).	Inspected the Incident Response Policy to determine that the company had security and privacy incident response policies in place. Inspected the HIPAA Compliance Policy to determine that the company had a policy in place to comply with HIPAA requirements.	No exceptions noted.
CA-72 - A business associate provides the company, as a business associate, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.	Inspected the Incident Response Policy to determine that the company had security and privacy incident response policies in place.	No exceptions noted.
CA-89 - The company, as a business associate, requires all business associates, following the discovery of a breach of unsecured protected health information, to notify the company of such breach. A breach is 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 due diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agents of the business associate (determined in accordance with the Federal common law of agency).	Inspected the Incident Response Policy to determine that the company had security and privacy incident response policies in place.	No exceptions noted.
CA-91 - Except in cases of a law enforcement delay (§ 164.412), a business associate provides the breach notification required by the company Breach Notification policy (§ 164.410(a)) without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach.	Inspected the signed Incident Response Policy for a sample of employees to determine employees agreed to the policy. Inspected the Incident Response Policy to determine that the company had security and privacy incident response policies in place.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-92 - A business associate's breach notification includes, 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 disclosed during the breach.	Inspected the Incident Response Policy to determine that the company had security and privacy incident response policies in place.	No exceptions noted.
CA-95 - The company, acting as a business associate, uses or discloses PHI only as permitted or required by its business associate agreement or as required by law, and makes required disclosures to the Secretary and to the covered entity or individual to support access requests.	Inspected the HIPAA Privacy Policy to determine that the company, acting as a business associate, used or disclosed Protected Health Information (PHI) only as permitted or required by its business associate agreement or as required by law, and made required disclosures to the Secretary and to the covered entity or individual to support access requests	No exceptions noted.
CA-96 - The company enters into business associate contracts that establish permitted and required uses and disclosures and obligate the business associate to safeguard PHI, report breaches, flow down terms to subcontractors, support individual rights, make records available to the Secretary, and return or destroy PHI at termination.	Inspected the Third-Party Policy to determine that the company had entered into business associate contracts that established permitted and required uses and disclosures of Protected Health Information (PHI) and obligated the business associate to safeguard PHI, report breaches, flow down applicable terms to subcontractors, support individual rights, make records available to the Secretary, and return or destroy PHI upon termination of the agreement	No exceptions noted.
CA-97 - The company, acting as a business associate, uses or discloses PHI for its own proper management and administration or legal responsibilities only as the contract permits and with required confidentiality and breach-notice assurances.	Inspected the Business Associate Agreement Template to determine that the company, acting as a business associate, used or disclosed Protected Health Information (PHI) for its own proper management and administration or to carry out its legal responsibilities only as permitted by the contract and with the required confidentiality and breach-notification assurances.	No exceptions noted.
CA-98 - The company, acting as a business associate, requires subcontractors that handle PHI on its behalf to enter into contracts subject to the same restrictions and conditions that apply to the company.	Inspected the list of vendors to determine that the company had written agreements in place with vendors and related third-parties. These agreements included confidentiality and privacy commitments applicable to that entity.	No exceptions noted.