Liquid Web, LLC

Data Center, Virtual Private Hosting, Dedicated Hosting, and Cloud Sites Services

Report on Management's Assertion on an Information Security Management System relevant to HIPAA/HITECH Objectives

November 1, 2023 - October 31, 2024

UHY LLP
www.uhy-us.com

Table of Contents

Section 1:

Independent Service Auditor's Report

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of:
Liquid Web, LLC
2703 Ena Dr.
Lansing, MI 48917

Scope

We have examined management of Liquid Web, LLC's ("Liquid Web") assertion that management has developed and implemented an information security management system over Liquid Web's Data Center, Virtual Private Hosting, Dedicated Hosting, and Cloud Sites services provided to user entities related to HIPAA and HITECH Security Rules and that the controls were suitably designed, implemented, and operated throughout the period November 1, 2023 to October 31, 2024 to provide reasonable assurance that Liquid Web's service commitments were achieved relevant to the HIPAA and HITECH Security Rules.

Liquid Web uses third-party service providers to host the client portal and provide physical security, internet connection, and environmental controls for the Arizona and Netherlands facilities. The information security management system was designed with the assumption that the third-party service providers have controls in place that are suitably designed and operating effectively, along with controls at Liquid Web, to achieve Liquid Web's service commitments. Our examination did not include the services provided by the third-party service providers, and we have not evaluated the suitability of the design or operating effectiveness of the third-party service providers' controls.

Service organization and service auditor responsibilities

Liquid Web's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. 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.

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

Inherent limitations

The information security management system 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 report users may consider important to meet their informational needs. There are inherent limitations in 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 and HITECH Security Rules. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Emphasis of Matter

As indicated in the testing approach on page 9, Liquid Web management designed and implemented controls pertinent to the HIPAA and HITECH Security Rules based on the in-scope services. The information security management system includes only the controls developed and implemented by Liquid Web to support management's service commitments to user entities related to the HIPAA and HITECH Security Rules. The information security management system includes a mapping of the pertinent controls to the applicable HIPAA and HITECH Security Rules. This mapping includes only Liquid Web's controls and does not include the user entity controls that are necessary for the user entity to meet the HIPAA and HITECH Security Rules.

Opinion

In our opinion Liquid Web's assertion that management has developed and implemented an information security management system over Liquid Web's Data Center, Virtual Private Hosting, Dedicated Hosting, and Cloud Sites services provided to user entities relevant to Liquid Web's service commitments related to the applicable HIPAA and HITECH Security Rules and that the controls were suitably designed, implemented, and operated effectively throughout the period November 1, 2023 to October 31, 2024, is fairly stated, in all material respects.

Restricted use

This report is intended solely for the information and use of management of Liquid Web and user entities of the Data Center, Virtual Private Hosting, Dedicated Hosting, and Cloud Sites services system and is not intended to be and should not be used by anyone other than these specified parties.

Farmington Hills, MI
March 28, 2025

Section 2:

Liquid Web, LLC Management's Assertion

Liquid Web, LLC Management's Assertion:

We have developed and implemented an information security management system over Liquid Web, LLC's ("Liquid Web") Data Center, Virtual Private Hosting, Dedicated Hosting, and Cloud Sites services provided to user entities relevant to the HIPAA and HITECH Security Rules.

Compliance with applicable HIPAA and HITECH Security Rules for user entities' environments is the responsibility of the user entity. User entities are responsible for designing and implementing internal controls, including monitoring controls at service providers, to address their compliance requirements. Liquid Web provides services that may impact or be necessary to support the user entities' compliance initiatives. As a result, the information security management system was developed to define Liquid Web's services commitments related to the HIPAA and HITECH Security Rules.

The information security management system was developed to identify relevant areas where Liquid Web's services provided to user entities may impact or be necessary to support the user entities' internal control related to the HIPAA and HITECH Security Rules and controls were implemented to address the identified areas related to the Data Center, Virtual Private Hosting, Dedicated Hosting, and Cloud Sites services provided by Liquid Web. The controls included in the system are only the controls Liquid Web believes are likely to be relevant to user entities' internal controls related to the HIPAA and HITECH Security Rules based on Liquid Web's service commitments.

Liquid Web uses third-party service providers to host the client portal and provide physical security, internet connection, and environmental controls for the Arizona and Netherlands facilities. The information security management system was designed with the assumption that the third-party service providers have controls in place that are suitably designed and operating effectively, along with controls at Liquid Web, to achieve Liquid Web's service commitments. The controls at the third-party service providers are not in-scope for management's assertion.

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

1) The information security management system over Liquid Web's Data Center, Virtual Private Hosting, Dedicated Hosting, and Cloud Sites services system was designed and implemented throughout the period November 1, 2023 to October 31, 2024 in order to meet the objectives of Liquid Web's services commitments related to the HIPAA and HITECH Security Rules.
2) The controls included in the information security management system were suitably designed throughout the period November 1, 2023 to October 31, 2024 to provide reasonable assurance that Liquid Web's service commitments related to the HIPAA and HITECH Security Rules would be achieved if the controls operated effectively during the period.
3) The controls included in the information security management system operated effectively throughout the period November 1, 2023 to October 31, 2024 to provide reasonable assurance that Liquid Web's service commitments related to the HIPAA and HITECH Security Rules were achieved.

Scott Arlen
Director, Network & Security Operations
Liquid Web, LLC

Section 3:

Independent Service Auditor's HIPAA Testing Approach and Key Findings

TESTING APPROACH

Our examination was conducted in accordance with attestation standards established by the AICPA. Our examination was conducted using the controls mapping provided by Liquid Web and the HIPAA and HITECH Security Rules.

Liquid Web management designed and implemented controls pertinent to the HIPAA and HITECH Security Rules based on the in-scope services. The information security management system includes only the controls developed and implemented by Liquid Web to support management's services commitments to user entities related to the HIPAA and HITECH Security Rules. The information security management system includes a mapping of the pertinent controls to the applicable HIPAA and HITECH Security Rules. This mapping includes only Liquid Web's controls and does not include the user entity controls that are necessary to meet the HIPAA and HITECH Security Rules.

Our tests of the control environment included the following procedures, to the extent we considered necessary: (a) a review of the organization's organizational structure, including the segregation of functional responsibilities, policy statements, accounting and processing manuals, personnel policies and the internal audit's policies; (b) discussions with management, operations, administrative and other personnel who are responsible for developing, ensuring adherence to and applying controls; and (c) observations of personnel in the performance of their assigned duties.

The control environment was considered in determining the nature, timing and extent of our testing of their controls to support our conclusions on the achievement of selected control objectives.

Our examination of the suitability of design and operational effectiveness of controls included the testing necessary, based upon our judgment, to evaluate whether adherence with those controls was sufficient to provide reasonable, but not absolute, assurance that the specified control objectives included below were achieved throughout the stated period.

KEY FINDINGS

All applicable controls were assessed based upon the documentation provided and results of testing work performed. A small number of HIPAA/HITECH regulations were determined to be not applicable ("N/A") to Liquid Web, given their operating structure. These areas are discussed fully in this section.

HIPAA Security Rule

We determined that the HIPAA Security Rule was relevant with respect to Liquid Web's operating structure. The HIPAA Security Rule requires that Administrative, Physical, and Technical safeguards be put in place and consistently monitored to ensure the security over electronic protected health information (ePHI).

Most of the Security Rule criteria were applicable and included in the scope of testing. Results of testing are provided below. Any criteria noted as "not applicable" are documented in our Testing Results provided below.

HIPAA Privacy Rule

We determined that the HIPAA Privacy Rule was relevant with respect to Liquid Web's operating structure, however, per the terms of the customer agreements, Liquid Web is not authorized to view customer ePHI. Customers are solely responsible for securing access to ePHI. Liquid Web is a data center and does not generate ePHI or make ePHI available to individuals.

HIPAA Electronic Health Record Technology (HITECH)

We determined that the HIPAA Electronic Health Record Technology (HITECH) regulations are relevant with respect to Liquid Web's operating structure as a Business Associate. Liquid Web provides Data Center, Virtual Private Hosting, Dedicated Hosting, and Cloud Sites services that does not generate ePHI or make ePHI available to individuals except under the terms of the customer agreements. Per the terms of the customer agreements, Liquid Web is not authorized to view customer PHI. Customers are solely responsible for securing access to ePHI. Therefore, controls related to technology used in providing health care services are not applicable.

Section 4:

HIPAA Requirements, Related Controls, and Tests of Controls

§164.308 Administrative Safeguards			
Service Organization Control Activity		**Test Performed by the Service Auditor**	**Test Results**
Risk Analysis			
§164.308(a)(1)(ii)(a)	**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.**		
Formal risk management policies and procedures have been implemented that define the company's risk assessment objectives including assessing operations, reporting, and compliance risks. Risk management policies and procedures are reviewed and updated by management on at least annual basis.		Inspected the Risk Assessment Policy and Risk Management Framework to verify that formal policies and procedures have been implemented that define the company's risk assessment objectives including assessing operations, reporting, and compliance risks. Inspected the Risk Assessment Policy and Risk Management Framework to verify that risk management policies and procedures are reviewed and updated by management on at least annual basis.	No exceptions noted.
A formal risk assessment is performed on at least an annual basis that includes the following components: o Reviewing company operational, financial, reporting, and compliance objectives and identifying risks that threaten the achievement of those risks o Consideration of fraud risk to achievement of the objectives o The identification of changes to the internal, external, legal, regulatory, or technological environments that could impact the Company's system of internal control o Assessment of third-party risk o Assigning a risk rating and action plans for how the company will respond to the identified risks		Inspected risk assessment documentation to verify that an assessment was performed on an annual basis and included the stated components.	No exceptions noted.
Risk Management			
§164.308(a)(1)(ii)(b)	**Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).**		
Formal risk management policies and procedures have been implemented that define the company's risk assessment objectives including assessing operations, reporting, and compliance risks. Risk management policies and procedures are reviewed and updated by management on at least annual basis.		Inspected the Risk Assessment Policy and Risk Management Framework to verify that formal policies and procedures have been implemented that define the company's risk assessment objectives including assessing operations, reporting, and compliance risks. Inspected the Risk Assessment Policy and Risk Management Framework to verify that risk management policies and procedures are reviewed and updated by management on at least annual basis.	No exceptions noted.

§164.308 Administrative Safeguards		
Service Organization Control Activity	**Test Performed by the Service Auditor**	**Test Results**
A formal risk assessment is performed on at least an annual basis that includes the following components: o Reviewing company operational, financial, reporting, and compliance objectives and identifying risks that threaten the achievement of those risks o Consideration of fraud risk to achievement of the objectives o The identification of changes to the internal, external, legal, regulatory, or technological environments that could impact the Company's system of internal control o Assessment of third-party risk o Assigning a risk rating and action plans for how the company will respond to the identified risks	Inspected risk assessment documentation to verify that an assessment was performed on an annual basis and included the stated components.	No exceptions noted.
Sanction Policy		
§164.308(a)(1)(ii)(c)	**Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.**	
A corrective action policy in place that defines the procedures and sanctions to be taken in the event of non-compliance with the organization's standards of conduct and information security policies.	Inspected the Employee Handbook to verify that a corrective action policy in place that defined the procedures and sanctions to be taken in the event of non-compliance with the company's standards of conduct and information security policies.	No exceptions noted.
Information System Activity Review		
§164.308(a)(1)(ii)(d)	**Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.**	
The organization uses an issue tracking system to record and monitor security and availability issues through resolution. Unusual or suspicious network activity is highlighted and forwarded to network administrators for investigation and resolution.	Inspected the issue tracking system to verify that the organization uses an issue tracking system to record and monitor security and availability issues through resolution. Inspected example issue tickets to verify that unusual or suspicious network activity is highlighted and forwarded to network administrators for investigation and resolution.	No exceptions noted.

§164.308 Administrative Safeguards		
Service Organization Control Activity	**Test Performed by the Service Auditor**	**Test Results**
Incident Outcomes and Action Review (IOAR) meetings are held monthly. IOAR meetings are a forum to evaluate control deficiencies, develop new control activities, track identified risks, and communicate relevant changes to internal controls and employee responsibilities.	Inspected Incident Outcomes and Action Review (IOAR) documentation for a sample of months to verify that meetings are held monthly and are a forum to evaluate control deficiencies, develop new control activities, track identified risks, and communicate relevant changes to internal controls and employee responsibilities.	No exceptions noted.
User access reviews are performed annually by the Department Heads to determine if access privileges are appropriate.	Inspected authentication system permissions audit documentation to verify that user access reviews are performed annually by the Department Heads to determine if access privileges are appropriate.	No exceptions noted.
Network monitoring tools are utilized to monitor network operations and provide real-time information on system performance and outages.	Inspected the network monitoring tools utilized by the organization and example alerts to verify that tools were used to monitor network operations and provide real-time information on system performance and outages.	No exceptions noted.
The badge access system logs successful and failed access attempts. Logs are retained for a minimum of 90 days.	Inspected badge system access log examples throughout the period to verify that the system logs successful and failed access attempts. Inspected historic access logs and the badge system access log retention settings to verify that logs are retained for a minimum of 90 days.	No exceptions noted.
The Infrastructure Team performs a monthly review of unused badges, failed badge access attempts, deleted and added badges, and changes to badge access.	Inspected completed Monthly Physical Security Reports for a sample of months during the attestation period to verify that the Infrastructure Team performs a monthly review of unused badges, failed badge access attempts, deleted and added badges, and changes to badge access.	No exceptions noted.
Security-related log-in events are logged and reviewed.	Inspected the log-in monitoring log to verify that security-related log-in events are logged and reviewed. Inquired with IT management to verify that security-related log-in events are reviewed by the company.	No exceptions noted.

§164.308 Administrative Safeguards			
Service Organization Control Activity		**Test Performed by the Service Auditor**	**Test Results**
Assigned Security Responsibility			
§164.308(a)(2)	**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.**		
The Security Team has been formally assigned the responsibility for information security within the organization.		Inspected the Information Security Policy to verify that the Security Team has been formally assigned the responsibility for information security within the company.	No exceptions noted.
Authorization and/or Supervision			
§164.308(a)(3)(ii)(a)	**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.**		
Authorized users are identified and authenticated via a unique user ID and password. Access to hosting-related systems and infrastructure is further restricted via SSH and two-factor authentication. User IDs are unique and passwords are encrypted.		Inspected network authentication screens and example network security event logs to verify that all authorized users are identified and authenticated via a unique user ID and password. Inspected network authentication screens to verify that access to hosting related systems and infrastructure is further restricted via SSH and two-factor authentication. Inspected the user access listing to verify that User IDs are unique. Inspected the authentication system encryption settings to verity that passwords are encrypted.	No exceptions noted.
Access to information is restricted based on job function and role utilizing minimum access required for job responsibilities.		Inspected user access lists and permissions listing to verify that access to information is restricted based on job function and role utilizing minimum access required for job responsibilities.	No exceptions noted.
User access for new employees is requested by the Human Resources/employee's manager through the Office IT department. The Office IT department assigns users to a group profile based on their role and department.		Inspected new hire provisioning documentation for a sample of new hires to verify that new user access is requested and approved by HR or the user's manager through the Office IT department. Inspected access permissions for a sample of new hires to verify that the Office IT Department assigned users to groups based on their department.	No exceptions noted.

§164.308 Administrative Safeguards		
Service Organization Control Activity	**Test Performed by the Service Auditor**	**Test Results**
Modifications to user access are requested by the employee's Department Head and approved by the Office IT department.	Inspected access modification request documentation for a sample of user access changes to verify that modifications to user access are requested by the employee's Department Head and approved by the Office IT department.	No exceptions noted.
Workforce Clearance Procedure		
§164.308(a)(3)(ii)(b)	**Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.**	
Background checks are conducted for new employees.	Inspected background check documentation for a sample of new hires to verify that background checks are conducted for new employees.	No exceptions noted.
Employees are required to read and agree to abide by the company's policies, rules, and regulations upon hire.	Inspected signed Employee Handbook acknowledgments for a sample of new hires to verify that employees are required to read and agree to abide by the company's policies, rules, and regulations upon hire.	No exceptions noted.
User access reviews are performed annually by the Department Heads to determine if access privileges are appropriate.	Inspected authentication system permissions audit documentation to verify that user access reviews are performed annually by the Department Heads to determine if access privileges are appropriate.	No exceptions noted.
The Infrastructure Team performs a monthly review of unused badges, failed badge access attempts, deleted and added badges, and changes to badge access.	Inspected completed Monthly Physical Security Reports for a sample of months during the attestation period to verify that the Infrastructure Team performs a monthly review of unused badges, failed badge access attempts, deleted and added badges, and changes to badge access.	No exceptions noted.
Establish Termination Procedures		
§164.308(a)(3)(ii)(c)	**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).**	
IT management completes a termination form and revokes system access as a component of the employee termination process.	Inspected termination forms for a sample of terminated employees to verify that IT management completes a termination form as a component of the employee termination process. Inspected termination documentation and user access listings to verify that IT management revokes system access as a component of the employee termination process.	No exceptions noted.
User access reviews are performed annually by the Department Heads to determine if access privileges are appropriate.	Inspected authentication system permissions audit documentation to verify that user access reviews are performed annually by the Department Heads to determine if access privileges are appropriate.	No exceptions noted.

§164.308 Administrative Safeguards		
Service Organization Control Activity	**Test Performed by the Service Auditor**	**Test Results**
The Infrastructure Team performs a monthly review of unused badges, failed badge access attempts, deleted and added badges, and changes to badge access.	Inspected completed Monthly Physical Security Reports for a sample of months during the attestation period to verify that the Infrastructure Team performs a monthly review of unused badges, failed badge access attempts, deleted and added badges, and changes to badge access.	No exceptions noted.
Isolating Healthcare Clearinghouse Functions		
§164.308(a)(4)(ii)(a)	**If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.**	
This criterion is not applicable to the organization as the organization is not a health care clearinghouse.		
Access Authorization		
§164.308(a)(4)(ii)(b)	**Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.**	
Access to information is restricted based on job function and role utilizing minimum access required for job responsibilities.	Inspected user access lists and permissions listing to verify that access to information is restricted based on job function and role utilizing minimum access required for job responsibilities.	No exceptions noted.
User access for new employees is requested by the Human Resources/employee's manager through the Office IT department. The Office IT department assigns users to a group profile based on their role and department.	Inspected new hire provisioning documentation for a sample of new hires to verify that new user access is requested and approved by HR or the user's manager through the Office IT department. Inspected access permissions for a sample of new hires to verify that the Office IT Department assigned users to groups based on their department.	No exceptions noted.
Modifications to user access are requested by the employee's Department Head and approved by the Office IT department.	Inspected access modification request documentation for a sample of user access changes to verify that modifications to user access are requested by the employee's Department Head and approved by the Office IT department.	No exceptions noted.

§164.308 Administrative Safeguards			
Service Organization Control Activity		**Test Performed by the Service Auditor**	**Test Results**
Access Establishment and Modification			
§164.308(a)(4)(ii)(c)	**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.**		
Access to information is restricted based on job function and role utilizing minimum access required for job responsibilities.		Inspected user access lists and permissions listing to verify that access to information is restricted based on job function and role utilizing minimum access required for job responsibilities.	No exceptions noted.
User access for new employees is requested by the Human Resources/employee's manager through the Office IT department. The Office IT department assigns users to a group profile based on their role and department.		Inspected new hire provisioning documentation for a sample of new hires to verify that new user access is requested and approved by HR or the user's manager through the Office IT department. Inspected access permissions for a sample of new hires to verify that the Office IT Department assigned users to groups based on their department.	No exceptions noted.
Modifications to user access are requested by the employee's Department Head and approved by the Office IT department.		Inspected access modification request documentation for a sample of user access changes to verify that modifications to user access are requested by the employee's Department Head and approved by the Office IT department.	No exceptions noted.
Security Reminders			
§164.308(a)(5)(ii)(a)	**Periodic security updates.**		
Information security policies are reviewed on an annual basis and updated as necessary.		Inspected the Information Security policy to verify that the policy is reviewed on an annual basis and updated as necessary.	No exceptions noted.
A formal information security training program has been implemented. Employees receive security awareness training upon hire and annually thereafter.		Inspected the security training program to verify that a formal information security training program has been implemented. Inspected security awareness training documentation for the sample of new hires and current employees to verify that employees receive security awareness training upon hire and annually thereafter.	No exceptions noted.
Status pages are in place and available to customers to communicate matters affecting customer services and the functioning of internal control.		Inspected the organization's status page to verify that status pages are in place and available to customers to communicate matters affecting customer services and the functioning of internal control.	No exceptions noted.

§164.308 Administrative Safeguards		
Service Organization Control Activity	**Test Performed by the Service Auditor**	**Test Results**
Access Establishment and Modification		
Development notes are sent out to employees periodically. The notes include any updates that have happened to systems within the company that could affect customers and employees.	Inspected development note examples issued throughout the attestation period to verify that the notes are sent out to employees periodically. Inspected development note examples issued throughout the attestation period to verify that the notes include any updates that have happened to systems within the company that could affect customers and employees.	No exceptions noted.
Protection from Malicious Software		
§164.308(a)(5)(ii)(b)	**Procedures for guarding against, detecting, and reporting malicious software.**	
Malware protection software is installed on all systems commonly affected by malicious software. Malware protection software is configured to update every 60 minutes and to run a weekly scan.	Inspected systems listings and malware protection software reports to verify that malware protection software is installed on all systems commonly affected by malicious software. Inspected malware protection software central management server settings to verify that malware protection software is configured to update every 60 minutes and to run a weekly scan.	No exceptions noted.
Network monitoring tools are utilized to monitor network operations and provide real-time information on system performance and outages.	Inspected the network monitoring tools utilized by the organization and example alerts to verify that tools were used to monitor network operations and provide real-time information on system performance and outages.	No exceptions noted.
An Intrusion Prevention System (IPS) is in place and sends alerts for high and critical severity vulnerabilities.	Inspected IPS settings and alert examples to verify that an IPS system was in place and sends alerts for high and critical severity vulnerabilities.	No exceptions noted.
A formal information security training program has been implemented. Employees receive security awareness training upon hire and annually thereafter.	Inspected the security training program to verify that a formal information security training program has been implemented. Inspected security awareness training documentation for the sample of new hires and current employees to verify that employees receive security awareness training upon hire and annually thereafter.	No exceptions noted.

§164.308 Administrative Safeguards		
Service Organization Control Activity	**Test Performed by the Service Auditor**	**Test Results**
Log-in Monitoring		
§164.308(a)(5)(ii)(c) **Procedures for monitoring log-in attempts and reporting discrepancies.**		
Formal procedures have been implemented for monitoring log-in attempts.	Inspected the Security Monitoring and Reporting policy to verify that formal procedures have been implemented for monitoring log-in attempts.	No exceptions noted.
Security-related log-in events are logged and reviewed.	Inspected the log-in monitoring log to verify that security-related log-in events are logged and reviewed. Inquired with IT management to verify that security-related log-in events are reviewed by the company.	No exceptions noted.
Password Management		
§164.308(a)(5)(ii)(d) **Procedures for creating, changing, and safeguarding passwords.**		
Authorized users are identified and authenticated via a unique user ID and password. Access to hosting-related systems and infrastructure is further restricted via SSH and two-factor authentication. User IDs are unique and passwords are encrypted.	Inspected network authentication screens and example network security event logs to verify that all authorized users are identified and authenticated via a unique user ID and password. Inspected network authentication screens to verify that access to hosting related systems and infrastructure is further restricted via SSH and two-factor authentication. Inspected the user access listing to verify that User IDs are unique. Inspected the authentication system encryption settings to verity that passwords are encrypted.	No exceptions noted.
The following password parameters are in place for the network and VPN: • Maximum Age: 90 days • Password History: 4 Passwords • Character Classes (Complexity): 3 required • Minimum Length: 8 Characters • Lockout Threshold: 6 attempts • Lockout Duration: 10 minutes	Inspected the global password policy for the IDM to verify that the stated password parameters were in place.	No exceptions noted.

§164.308 Administrative Safeguards		
Service Organization Control Activity	**Test Performed by the Service Auditor**	**Test Results**
Network authentication is controlled via redundant authentication servers. Access to the servers is restricted to authorized administrators.	Inspected configurations showing the redundant authentication servers to verify that network authentication is controlled via redundant authentication servers. Inspected user access groups and permissions to verify that authentication servers are controlled by the network engineering and system operations groups.	No exceptions noted.
Encryption keys are utilized for authenticating to the organization's network. Encryption keys are generated randomly via an automated script.	Inspected authentication server encryption settings to verify that encryption keys were used for authentication to the network. Inspected the key generation script to verify that an automated script was used to generate authentication server encryption keys.	No exceptions noted.
A formal information security training program has been implemented. Employees receive security awareness training upon hire and annually thereafter.	Inspected the security training program to verify that a formal information security training program has been implemented. Inspected security awareness training documentation for the sample of new hires and current employees to verify that employees receive security awareness training upon hire and annually thereafter.	No exceptions noted.
Response and Reporting		
§164.308(a)(6)(ii)	**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.**	
A formal Incident Response Plan is in place that documents the process for identification, evaluation, response, and resolution. Additionally, the plan includes procedures for notifying the appropriate personnel and customers.	Inspected the Incident Management Plan to verify that a formal Incident Response Plan is in place that documents the process for identification, evaluation, response, resolution, and notification procedures.	No exceptions noted.
The organization uses an issue tracking system to record and monitor security and availability issues through resolution. Unusual or suspicious network activity is highlighted and forwarded to network administrators for investigation and resolution.	Inspected the issue tracking system to verify that the organization uses an issue tracking system to record and monitor security and availability issues through resolution. Inspected example issue tickets to verify that unusual or suspicious network activity is highlighted and forwarded to network administrators for investigation and resolution.	No exceptions noted.

§164.308 Administrative Safeguards		
Service Organization Control Activity	**Test Performed by the Service Auditor**	**Test Results**
Incident Outcomes and Action Review (IOAR) meetings are held monthly. IOAR meetings are a forum to evaluate control deficiencies, develop new control activities, track identified risks, and communicate relevant changes to internal controls and employee responsibilities.	Inspected Incident Outcomes and Action Review (IOAR) documentation for a sample of months to verify that meetings are held monthly and are a forum to evaluate control deficiencies, develop new control activities, track identified risks, and communicate relevant changes to internal controls and employee responsibilities.	No exceptions noted.
Data Backup Plan		
§164.308(a)(7)(ii)(a)	**Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.**	
This criterion is not applicable to the organization as the organization does not maintain or access ePHI for customers.		
Disaster Recovery Plan		
§164.308(a)(7)(ii)(b)	**Establish (and implement as needed) procedures to restore any loss of data.**	
Formal business continuity and disaster response plans are in place that outline steps to be taken to continue services and respond to disasters. The plans are reviewed annually and updated as necessary.	Inspected business continuity and disaster response plans to verify that plans are in place that outline steps to be taken to continue services and respond to disasters. Inspected business continuity and disaster response plans to verify that plans are reviewed annually and updated as necessary.	No exceptions noted.
Tabletop tests of system redundancy are completed to ensure the system remains available to customers at least annually.	Inspected tabletop system redundancy testing documentation to verify tabletop tests of system redundancy are completed to ensure the system remains available to customers at least annually.	No exceptions noted.
Critical internal system and infrastructure code backups are run on at least a daily basis to enable recovery of data.	Inspected backup schedules to verify that critical internal system and infrastructure code backups are run on an at least daily basis to enable recovery of data.	No exceptions noted.
Code backup systems generate backup logs and send alerts for failed backups to systems personnel for review.	Inspected backup log settings to verify that code backup systems generate backup logs. Inspected backup alert settings and examples to verify that code backup systems send alerts for failed backups to systems personnel for review.	No exceptions noted.
Code backups are stored at a secondary data center to provide additional recoverability.	Inspected backup storage settings to verify that code backups are stored at a secondary data center to provide additional recoverability.	No exceptions noted.

§164.308 Administrative Safeguards		
Service Organization Control Activity	**Test Performed by the Service Auditor**	**Test Results**
Critical internal system and infrastructure database backups run on an at least daily basis to enable recovery of data.	Inspected backup schedules to verify that critical internal system and infrastructure database backups run on an at least daily basis to enable recovery of data.	No exceptions noted.
Database backup systems generate backup logs and send alerts for failed backups to systems personnel for review.	Inspected backup log settings to verify that database backup systems generate backup logs. Inspected backup alert settings and examples to verify that database backup systems send alerts for failed backups to systems personnel for review.	No exceptions noted.
Database backups are stored at a secondary data center to provide additional recoverability.	Inspected backup storage settings to verify that database backups are stored at a secondary data center to provide additional recoverability.	No exceptions noted.
Emergency Mode Operation Plan		
§164.308(a)(7)(ii)(c)	**Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.**	
Formal business continuity and disaster response plans are in place that outline steps to be taken to continue services and respond to disasters. The plans are reviewed annually and updated as necessary.	Inspected business continuity and disaster response plans to verify that plans are in place that outline steps to be taken to continue services and respond to disasters. Inspected business continuity and disaster response plans to verify that plans are reviewed annually and updated as necessary.	No exceptions noted.
Tabletop tests of system redundancy are completed to ensure the system remains available to customers at least annually.	Inspected tabletop system redundancy testing documentation to verify tabletop tests of system redundancy are completed to ensure the system remains available to customers at least annually.	No exceptions noted.

§164.308 Administrative Safeguards		
Service Organization Control Activity	**Test Performed by the Service Auditor**	**Test Results**
Testing and Revision Procedure		
§164.308(a)(7)(ii)(d)	**Implement procedures for periodic testing and revision of contingency plans.**	
Formal business continuity and disaster response plans are in place that outline steps to be taken to continue services and respond to disasters. The plans are reviewed annually and updated as necessary.	Inspected business continuity and disaster response plans to verify that plans are in place that outline steps to be taken to continue services and respond to disasters. Inspected business continuity and disaster response plans to verify that plans are reviewed annually and updated as necessary.	No exceptions noted.
Tabletop tests of system redundancy are completed to ensure the system remains available to customers at least annually.	Inspected tabletop system redundancy testing documentation to verify tabletop tests of system redundancy are completed to ensure the system remains available to customers at least annually.	No exceptions noted.
Application and Data Criticality Analysis		
§164.308(a)(7)(ii)(e)	**Assess the relative criticality of specific applications and data in support of other contingency plan components.**	
A formal risk assessment is performed on at least an annual basis that includes the following components: o Reviewing company operational, financial, reporting, and compliance objectives and identifying risks that threaten the achievement of those risks o Consideration of fraud risk to achievement of the objectives o The identification of changes to the internal, external, legal, regulatory, or technological environments that could impact the Company's system of internal control o Assessment of third-party risk o Assigning a risk rating and action plans for how the company will respond to the identified risks	Inspected risk assessment documentation to verify that an assessment was performed on an annual basis and included the stated components.	No exceptions noted.
Incident Outcomes and Action Review (IOAR) meetings are held monthly. IOAR meetings are a forum to evaluate control deficiencies, develop new control activities, track identified risks, and communicate relevant changes to internal controls and employee responsibilities.	Inspected Incident Outcomes and Action Review (IOAR) documentation for a sample of months to verify that meetings are held monthly and are a forum to evaluate control deficiencies, develop new control activities, track identified risks, and communicate relevant changes to internal controls and employee responsibilities.	No exceptions noted.

§164.308 Administrative Safeguards			
Service Organization Control Activity		**Test Performed by the Service Auditor**	**Test Results**
Evaluation			
§164.308(a)(8)	**Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.**		
A formal risk assessment is performed on at least an annual basis that includes the following components: o Reviewing company operational, financial, reporting, and compliance objectives and identifying risks that threaten the achievement of those risks o Consideration of fraud risk to achievement of the objectives o The identification of changes to the internal, external, legal, regulatory, or technological environments that could impact the Company's system of internal control o Assessment of third-party risk o Assigning a risk rating and action plans for how the company will respond to the identified risks		Inspected risk assessment documentation to verify that an assessment was performed on an annual basis and included the stated components.	No exceptions noted.
Quarterly external network assessments are performed to identify and address vulnerabilities and changes in the environment that may impact the security and availability of the system. The results of the assessments are communicated to IT management in a timely manner for review. Remediation efforts of issues found are documented by IT management.		Inspected completed external vulnerability scans and remediation documentation for each quarter during the attestation period to verify that quarterly external vulnerability scans were conducted, vulnerabilities were remediated, and results were communicated to IT management timely.	No exceptions noted.
Incident Outcomes and Action Review (IOAR) meetings are held monthly. IOAR meetings are a forum to evaluate control deficiencies, develop new control activities, track identified risks, and communicate relevant changes to internal controls and employee responsibilities.		Inspected Incident Outcomes and Action Review (IOAR) documentation for a sample of months to verify that meetings are held monthly and are a forum to evaluate control deficiencies, develop new control activities, track identified risks, and communicate relevant changes to internal controls and employee responsibilities.	No exceptions noted.

§164.308 Administrative Safeguards		
Service Organization Control Activity	**Test Performed by the Service Auditor**	**Test Results**
Business Associate Contracts and Other Arrangements		
§164.308(b)(1)	**A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.**	
This criterion is not applicable to the organization as the organization is not a covered entity and does not have business associates.		
Business Associate Contracts and Other Arrangements		
§164.308(b)(2)	**A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.**	
This criterion is not applicable to the organization as the organization is not a covered entity and does not have business associates.		
Written Contract or Other Arrangement		
§164.308(b)(3):	**Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).**	
This criterion is not applicable to the organization as the organization is not a covered entity and does not have business associates.		

§164.310 Physical Safeguards			
Service Organization Control Activity		**Test Performed by the Service Auditor**	**Test Results**
Contingency Operations			
§164.310(a)(2)(i)	**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.**		
Formal business continuity and disaster response plans are in place that outline steps to be taken to continue services and respond to disasters. The plans are reviewed annually and updated as necessary.		Inspected business continuity and disaster response plans to verify that plans are in place that outline steps to be taken to continue services and respond to disasters. Inspected business continuity and disaster response plans to verify that plans are reviewed annually and updated as necessary.	No exceptions noted.
Tabletop tests of system redundancy are completed to ensure the system remains available to customers at least annually.		Inspected tabletop system redundancy testing documentation to verify tabletop tests of system redundancy are completed to ensure the system remains available to customers at least annually.	No exceptions noted.
Facility Security Plan			
§164.310(a)(2)(ii)	**Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.**		
Formal policies and procedures are in place to guide personnel in the organization's physical security protocols.		Inspected the Physical Security and Badge Access policies to verify that documented physical security policies and procedures were in place to communicate physical security standards to personnel. Inspected the company wiki to verify that the Physical Security and Badge Access policies was made available to relevant personnel.	No exceptions noted.
Surveillance cameras are in place to monitor and record activity throughout the facilities, work areas, and data centers. Surveillance video is retained for a minimum of 90 days.		Observed the surveillance cameras throughout the facilities, work areas, and data centers during onsite walkthrough to verify that cameras are in place to monitor and record activity. Observed historic surveillance video to verify that video is retained for a minimum of 90 days. Inspected surveillance cameras settings to verify that video is retained for a minimum of 90 days.	No exceptions noted.

§164.310 Physical Safeguards		
Service Organization Control Activity	**Test Performed by the Service Auditor**	**Test Results**
Visitors are required to present a valid photo ID and are provided a visitor badge upon entry to the facilities. Visitors are escorted for the duration of their visit.	Observed the visitor check in process during onsite walkthroughs to verify that visitors are required to present a valid photo ID and are provided a visitor badge upon entry to the facilities. Observed visitors being escorted during onsite walkthroughs to verify that to verify that visitors are escorted for the duration of their visit.	No exceptions noted.
Access to the data center is restricted to technical staff and personnel with a business need to access the data center.	Observed the data access restrictions during onsite walkthroughs to verify that access is restricted to technical staff and personnel with a business need to access the data center. Inspected badge system access listings to verify that access is restricted to technical staff and personnel with a business need to access the data center.	No exceptions noted.
Access to telecom and central switching equipment is restricted within the data centers to authorized personnel through the use of a badge access system.	Observed the equipment access restrictions during onsite walkthroughs to verify that access to telecom and central switching equipment is restricted within the data centers to authorized personnel through the use of a badge access system.	No exceptions noted.
Administrative access to the in-scope (Firewalls, badge access system, IPS, network, authentication systems, VPN, etc.) systems is restricted to authorized system administration personnel.	Inspected user access listings to the in-scope systems to verify that the administrative access is restricted to authorized system administration personnel.	No exceptions noted.
The Infrastructure Team performs a monthly review of unused badges, failed badge access attempts, deleted and added badges, and changes to badge access.	Inspected completed Monthly Physical Security Reports for a sample of months during the attestation period to verify that the Infrastructure Team performs a monthly review of unused badges, failed badge access attempts, deleted and added badges, and changes to badge access.	No exceptions noted.

§164.310 Physical Safeguards			
Service Organization Control Activity		**Test Performed by the Service Auditor**	**Test Results**
Access Control and Validation Procedures			
§164.310(a)(2)(iii)	**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.**		
Formal policies and procedures are in place to guide personnel in the organization's physical security protocols.		Inspected the Physical Security and Badge Access policies to verify that documented physical security policies and procedures were in place to communicate physical security standards to personnel. Inspected the company wiki to verify that the Physical Security and Badge Access policies was made available to relevant personnel.	No exceptions noted.
Surveillance cameras are in place to monitor and record activity throughout the facilities, work areas, and data centers. Surveillance video is retained for a minimum of 90 days.		Observed the surveillance cameras throughout the facilities, work areas, and data centers during onsite walkthrough to verify that cameras are in place to monitor and record activity. Observed historic surveillance video to verify that video is retained for a minimum of 90 days. Inspected surveillance cameras settings to verify that video is retained for a minimum of 90 days.	No exceptions noted.
Visitors are required to present a valid photo ID and are provided a visitor badge upon entry to the facilities. Visitors are escorted for the duration of their visit.		Observed the visitor check in process during onsite walkthroughs to verify that visitors are required to present a valid photo ID and are provided a visitor badge upon entry to the facilities. Observed visitors being escorted during onsite walkthroughs to verify that to verify that visitors are escorted for the duration of their visit.	No exceptions noted.
Access to the data center is restricted to technical staff and personnel with a business need to access the data center.		Observed the data access restrictions during onsite walkthroughs to verify that access is restricted to technical staff and personnel with a business need to access the data center. Inspected badge system access listings to verify that access is restricted to technical staff and personnel with a business need to access the data center.	No exceptions noted.

§164.310 Physical Safeguards			
Service Organization Control Activity		**Test Performed by the Service Auditor**	**Test Results**
Access to telecom and central switching equipment is restricted within the data centers to authorized personnel through the use of a badge access system.		Observed the equipment access restrictions during onsite walkthroughs to verify that access to telecom and central switching equipment is restricted within the data centers to authorized personnel through the use of a badge access system.	No exceptions noted.
Administrative access to the in-scope (Firewalls, badge access system, IPS, network, authentication systems, VPN, etc.) systems is restricted to authorized system administration personnel.		Inspected user access listings to the in-scope systems to verify that the administrative access is restricted to authorized system administration personnel.	No exceptions noted.
The Infrastructure Team performs a monthly review of unused badges, failed badge access attempts, deleted and added badges, and changes to badge access.		Inspected completed Monthly Physical Security Reports for a sample of months during the attestation period to verify that the Infrastructure Team performs a monthly review of unused badges, failed badge access attempts, deleted and added badges, and changes to badge access.	No exceptions noted.
Maintain Maintenance Records			
§164.310(a)(2)(iv)	**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).**		
The Infrastructure Team performs a monthly review of unused badges, failed badge access attempts, deleted and added badges, and changes to badge access.		Inspected completed Monthly Physical Security Reports for a sample of months during the attestation period to verify that the Infrastructure Team performs a monthly review of unused badges, failed badge access attempts, deleted and added badges, and changes to badge access.	No exceptions noted.
Workstation Use			
§164.310(b)	**Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.**		
A formal acceptable use policy is in place and available to all employees via the organization's Internal Wiki.		Inspected the Acceptable Use policy to verify that a formal acceptable use policy is in place and available to all employees via the organization's Internal Wiki.	No exceptions noted.
Access to the facilities, work areas, and data centers is restricted to authorized personnel through the use of a badge access system.		Observed the entrances and exits to the facilities, work areas, and data centers during onsite walkthrough to verify that access is restricted to authorized personnel through the use of a badge access system.	No exceptions noted.

§164.310 Physical Safeguards			
Service Organization Control Activity		**Test Performed by the Service Auditor**	**Test Results**
Workstation Security			
§164.310(c)	**Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.**		
Surveillance cameras are in place to monitor and record activity throughout the facilities, work areas, and data centers. Surveillance video is retained for a minimum of 90 days.		Observed the surveillance cameras throughout the facilities, work areas, and data centers during onsite walkthrough to verify that cameras are in place to monitor and record activity. Observed historic surveillance video to verify that video is retained for a minimum of 90 days. Inspected surveillance cameras settings to verify that video is retained for a minimum of 90 days.	No exceptions noted.
Visitors are required to present a valid photo ID and are provided a visitor badge upon entry to the facilities. Visitors are escorted for the duration of their visit.		Observed the visitor check in process during onsite walkthroughs to verify that visitors are required to present a valid photo ID and are provided a visitor badge upon entry to the facilities. Observed visitors being escorted during onsite walkthroughs to verify that to verify that visitors are escorted for the duration of their visit.	No exceptions noted.
Access to the data center is restricted to technical staff and personnel with a business need to access the data center.		Observed the data access restrictions during onsite walkthroughs to verify that access is restricted to technical staff and personnel with a business need to access the data center. Inspected badge system access listings to verify that access is restricted to technical staff and personnel with a business need to access the data center.	No exceptions noted.
Access to telecom and central switching equipment is restricted within the data centers to authorized personnel through the use of a badge access system.		Observed the equipment access restrictions during onsite walkthroughs to verify that access to telecom and central switching equipment is restricted within the data centers to authorized personnel through the use of a badge access system.	No exceptions noted.

§164.310 Physical Safeguards			
Service Organization Control Activity		**Test Performed by the Service Auditor**	**Test Results**
The badge access system logs successful and failed access attempts. Logs are retained for a minimum of 90 days.		Inspected badge system access log examples throughout the period to verify that the system logs successful and failed access attempts. Inspected historic access logs and the badge system access log retention settings to verify that logs are retained for a minimum of 90 days.	No exceptions noted.
Disposal			
§164.310(d)(2)(i)	**Implement policies and procedures to address the final disposition of electronic protected health information and/or the hardware or electronic media on which it is stored.**		
Decommissioned hardware is tracked through an inventory management system and stored in a physically secured area until sanitization and/or destruction.		Inspected the inventory management system to verify that decommissioned hardware is tracked through an inventory management system. Observed the physical security of the decommissioned hardware storage area during onsite walkthroughs to verify that decommissioned hardware is stored in a physically secured area until sanitization and/or destruction.	No exceptions noted.
Media Re-use			
§164.310(d)(2)(ii)	**Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.**		
A hardware sanitization policy is in place outlines the procedures for the pre-disposal data sanitization of hardware.		Inspected the Hardware Sanitization policy to verify that a policy was place that outlines the procedures for the pre-disposal data sanitization of hardware.	No exceptions noted.
Decommissioned hardware is tracked through an inventory management system and stored in a physically secured area until sanitization and/or destruction.		Inspected the inventory management system to verify that decommissioned hardware is tracked through an inventory management system. Observed the physical security of the decommissioned hardware storage area during onsite walkthroughs to verify that decommissioned hardware is stored in a physically secured area until sanitization and/or destruction.	No exceptions noted.

§164.310 Physical Safeguards			
Service Organization Control Activity		**Test Performed by the Service Auditor**	**Test Results**
Accountability			
§164.310(d)(2)(iii)	**Maintain a record of the movements of hardware and electronic media and any person responsible therefore.**		
A hardware sanitization policy is in place outlines the procedures for the pre-disposal data sanitization of hardware.		Inspected the Hardware Sanitization policy to verify that a policy was place that outlines the procedures for the pre-disposal data sanitization of hardware.	No exceptions noted.
The organization maintains a formal system inventory that tracks hardware within the environment.		Inspected the system inventory to verify that the organization maintains a formal system inventory that tracks hardware within the environment.	No exceptions noted.
Data Backup and Storage Procedures			
§164.310(d)(2)(iv)	**Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.**		
This criterion is not applicable to the organization as the organization does not maintain or access ePHI for customers.			

§164.312 Technical Safeguards			
Service Organization Control Activity		**Test Performed by the Service Auditor**	**Test Results**
Unique User Identification			
§164.312(a)(2)(i)	**Assign a unique name and/or number for identifying and tracking user identity.**		
Authorized users are identified and authenticated via a unique user ID and password. Access to hosting-related systems and infrastructure is further restricted via SSH and two-factor authentication. User IDs are unique and passwords are encrypted.		Inspected network authentication screens and example network security event logs to verify that all authorized users are identified and authenticated via a unique user ID and password. Inspected network authentication screens to verify that access to hosting related systems and infrastructure is further restricted via SSH and two-factor authentication. Inspected the user access listing to verify that User IDs are unique. Inspected the authentication system encryption settings to verity that passwords are encrypted.	No exceptions noted.
Client portal authentication requires a user name and password. The connect is secured via TLS connections to protect the confidentiality and integrity of data passing over public networks.		Inspected the portal authentication to verify that the client portal authentication requires a user name and password. Inspected the portal TLS certificate to verify that the connection is secured via TLS to protect the confidentiality and integrity of data passing over public networks.	No exceptions noted.
Emergency Access Procedure			
§164.312(a)(2)(ii)	**Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.**		
This criterion is not applicable to the organization as the organization does not maintain or access ePHI for customers.			
Automatic Logoff			
§164.312(a)(2)(iii)	**Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.**		
A formal General Workstation Guidelines policy is in place that outlines the procedures for securing workstations.		Inspected the General Workstation Guidelines policy to verify that a policy is in place that outlines the procedures for securing workstations.	No exceptions noted.
Workstations are configured with a password protected screen saver that is activated after a predetermined time of inactivity.		Inspected the global workstation security settings to verify that workstations are configured with a password protected screen saver that is activated after a predetermined time of inactivity.	No exceptions noted.

§164.312 Technical Safeguards			
Service Organization Control Activity		**Test Performed by the Service Auditor**	**Test Results**
Encryption and Decryption			
§164.312(a)(2)(iv)	**Implement a mechanism to encrypt and decrypt electronic protected health information.**		
This criterion is not applicable to the organization as the organization does not maintain or access ePHI for customers.			
Audit Controls			
§164.312(b)	**Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.**		
This criterion is not applicable to the organization as the organization does not maintain or access ePHI for customers.			
Mechanism to Authenticate ePHI			
§164.312(c)(2)	**Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.**		
This criterion is not applicable to the organization as the organization does not maintain or access ePHI for customers.			
Person or Entity Authentication			
§164.312(d)	**Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed**		
This criterion is not applicable to the organization as the organization does not maintain or access ePHI for customers.			
Integrity Controls			
§164.312(e)(2)(i)	**Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.**		
This criterion is not applicable to the organization as the organization does not maintain or access ePHI for customers.			
Encryption			
§164.312(e)(2)(ii)	**Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.**		
This criterion is not applicable to the organization as the organization does not maintain or access ePHI for customers.			