INDEPENDENT PRACTITIONER'S REPORT

LIQUID WEB, LLC

Co-Location, Web Hosting, and Network Infrastructure Services

Report on Management's Assertion on

Compliance with HIPAA/HITECH Criteria

For the Period
July 1, 2017 – June 30, 2018

UHY LLP
Certified Public Accountants

LIQUID WEB, LLC

Report on Management's Assertion on Compliance with HIPAA/HITECH Criteria

TABLE OF CONTENTS

UHY LLP
Certified Public Accountants

I. INDEPENDENT SERVICE PRACTITIONER'S REPORT

To the Management of Liquid Web, LLC

We have examined management's assertion that Liquid Web, LLC ("Liquid Web") is compliant with applicable HIPAA and HITECH regulations throughout the period July 1, 2017 through June 30, 2018. Management is responsible for Liquid Web's compliance with these regulations. 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 American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence supporting Liquid Web's compliance with applicable HIPAA and HITECH regulations and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion. Our examination does not provide a legal determination on Liquid Web's compliance with specified requirements.

In our opinion, management's assertion referred to above is fairly stated, in all material respects, based on applicable HIPAA and HITECH regulations.

This report is intended solely for the information and use of management of Liquid Web and its institutional clients and is not intended to be and should not be used by anyone other than these specified parties.

UHY LLP

Farmington Hills, Michigan
December 7, 2018

II. MANAGEMENT'S ASSERTION

Liquid Web's Assertion:

Liquid Web confirms that to the best of our knowledge and belief, the controls to meet the HIPAA and HITECH Security and Privacy Rule were suitably designed and operated effectively throughout the period July 1, 2017 through June 30, 2018 to achieve those control objectives. The criteria we used in making this assertion were that

i. The risks that threaten the achievement of the controls related to the HIPAA and HITECH criteria have been identified by Liquid Web.

ii. The controls related to the HIPAA and HITECH criteria would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the HIPAA and HITECH criteria from being achieved.

III. LIQUID WEB HIPAA TESTING APPROACH

We conducted our examination using the Office of Civil Rights (OCR) Audit Program Protocol as a guide. As a result of the American Recovery and Reinvestment Act of 2009, the Department of Health and Human Services (HHS) is required to perform periodic audits of covered entities and business associates and determine whether they are complying with HIPAA requirements. OCR released their Audit Program Protocol as a benchmark of best practice standards and procedures with regard to HIPAA audits.

Our testing involved the use of best practice audit procedures developed by OCR. See Section IV – Key Findings and Summary of Testing Results for a summary of the HIPAA and HITECH regulations determined to be relevant to Liquid Web and for a summary of our testing results.

We inspected Liquid Webs Data Protection Policies and Procedures Manual, as well as their Business Continuity Plan, Security Training Materials, and other documents. We inquired of management when appropriate. We also performed additional testing in accordance with the audit procedures developed by OCR in their Audit Program Protocol. We leveraged testing performed during our Systems and Organizational Control attestations, which included a Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting (SOC 1), a Report on Controls at a Service Organization Relevant to Security and Availability (SOC 2), and a Trust Services Report for Service Organizations Relevant to Security and Availability (SOC 3).

IV. KEY FINDINGS, SUMMARY OF TESTING RESULTS

Liquid Web was determined to be fully compliant with applicable HIPAA/HITECH regulations. All applicable controls were assessed based upon the documentation provided and results of testing work performed.

A 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. Certain exceptions to this general rule were determined and noted. The reasons why these items are 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. 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. Liquid Web is a data center and does not generate ePHI or make ePHI available to individuals except under the terms of the customer agreements. Therefore, controls related to technology used in providing health care services are not applicable.

HIPAA Established Performance Criteria		Implementation Specification / Key Activity	Tests of Operating Effectiveness	Test Results
§164.308	**Administrative Safeguards**			
§164.308(a)(1)	**Security Management Process**			
§164.308(a)(1)(i)	Implement policies and procedures to prevent, detect, contain, and correct security violations.	Security Management Process	Inspected the implemented policies and procedures addressing preventing, detecting, containing, and correct security violations.	HIPAA Compliant
§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.	Risk Analysis	Inspected the risk assessment process and annual completed risk assessment.	HIPAA Compliant
§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).	Risk Management	Inspected the risk assessment process and annual completed risk assessment.	HIPAA Compliant
§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.	Sanction Policy	Inspected the company sanction policy addressing actions to be taken regarding violations of company policies.	HIPAA Compliant
§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.	Information System Activity Review	Inspected documentation of physical and logical access and activity monitoring, documentation, resolution, and reporting.	HIPAA Compliant

HIPAA Established Performance Criteria		Implementation Specification / Key Activity	Tests of Operating Effectiveness	Test Results
§164.308(a)(2)	**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.	Assigned Security Responsibility	Inspected the Information Security Policy including the formal assignment of responsibility for development and implementation of required policies and procedures.	HIPAA Compliant
§164.308(a)(3)	**Workforce Security**			
§164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	Workforce Security	Inspected company policies, procedures, and implemented access controls and restrictions at the company.	HIPAA Compliant
§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.	Authorization and/or Supervision	Inspected company policies, procedures, access request documentation, implemented access controls and restrictions at the company.	HIPAA Compliant
§164.308(a)(3)(ii)(B)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Workforce Clearance Procedure	Inspected company screening procedures, performance reviews, and access reviews.	HIPAA Compliant
§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).	Establish Termination Procedures	Inspected termination documentation for a sample of employees noting that logical and physical access was terminated timely.	HIPAA Compliant

HIPAA Established Performance Criteria		Implementation Specification / Key Activity	Tests of Operating Effectiveness	Test Results
§164.308(a)(4)	**Information Access Management**			
§164.308(a)(4)(i)	Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	Information Access Management	Inspected company policies, procedures, access request documentation for a sample of new hires, access modification request documentation, and access restrictions at the company.	HIPAA Compliant
§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.	Isolating Healthcare Clearinghouse Functions	This criteria is not applicable to Liquid Web as Liquid Web is not a health care clearing house.	Not Applicable
§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 Authorization	Inspected company policies, procedures, access request documentation for a sample of new hires, access modification request documentation for a sample of user access modifications, and access restrictions at the company.	HIPAA Compliant
§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 Establishment and Modification	Inspected company policies, procedures, access request documentation for a sample of new hires, access modification request documentation for a sample of user access modifications, and access restrictions at the company.	HIPAA Compliant

HIPAA Established Performance Criteria		Implementation Specification / Key Activity	Tests of Operating Effectiveness	Test Results
§164.308(a)(5)	**Security Awareness Training**			
§164.308(a)(5)(i)	Implement a security awareness and training program for all members of its workforce (including management).	Security Awareness and Training	Inspected the company's security awareness training program.	HIPAA Compliant
§164.308(a)(5)(ii)(A)	Periodic security updates.	Security Reminders	Inspected the security update process and completed new hire and annual training documentation for a sample of employees.	HIPAA Compliant
§164.308(a)(5)(ii)(B)	Procedures for guarding against, detecting, and reporting malicious software.	Protection from Malicious Software	Inspected firewall, Intrusion Prevention Systems, malware protection software, and security training documentation for a sample of new hires and current employees.	HIPAA Compliant
§164.308(a)(5)(ii)(C)	Procedures for monitoring log-in attempts and reporting discrepancies.	Log-in Monitoring	Inspected the company's policies and monitoring procedures covering security-related events including log-in attempts.	HIPAA Compliant
§164.308(a)(5)(ii)(D)	Procedures for creating, changing, and safeguarding passwords.	Password Management	Inspected authentication documentation, including password rotation, encryption, and security. Inspected security training documentation for a sample of new hires and current employees.	HIPAA Compliant
§164.308(a)(6)	**Security Incident Procedures**			
§164.308(a)(6)(i)	Implement policies and procedures to address security incidents.	Security Incident Procedures	Inspected the company's Incident Management Plan documentation.	HIPAA Compliant
§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.	Response and Reporting	Inspected the company's Incident Management Plan and examples of security incident tickets.	HIPAA Compliant

HIPAA Established Performance Criteria		Implementation Specification / Key Activity	Tests of Operating Effectiveness	Test Results
§164.308(a)(7)	**Contingency Plan**			
§164.308(a)(7)(i)	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	Contingency Plan	Inspected the results of the annual system redundancy and disaster recovery testing.	HIPAA Compliant
§164.308(a)(7)(ii)(A)	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	Data Backup Plan	This criteria is not applicable to Liquid Web as Liquid Web does not maintain ePHI for customers.	Not Applicable
§164.308(a)(7)(ii)(B)	Establish (and implement as needed) procedures to restore any loss of data.	Disaster Recovery Plan	Inspected disaster recovery, backup schedule, backup logs, and backup storage documentation for internal systems and infrastructure.	HIPAA Compliant
§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.	Emergency Mode Operation Plan	Inspected the results of the annual system redundancy and disaster recovery testing.	HIPAA Compliant
§164.308(a)(7)(ii)(D)	Implement procedures for periodic testing and revision of contingency plans.	Testing and Revision Procedure	Inspected the results of the annual system redundancy and disaster recovery testing.	HIPAA Compliant
§164.308(a)(7)(ii)(E)	Assess the relative criticality of specific applications and data in support of other contingency plan components.	Application and Data Criticality Analysis	Inspected the results of the company's annual risk assessment.	HIPAA Compliant

HIPAA Established Performance Criteria		Implementation Specification / Key Activity	Tests of Operating Effectiveness	Test Results
§164.308(a)(8)	**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.	Evaluation	Inspected the results of the company's annual risk assessment.	HIPAA Compliant
§164.310	**Physical Safeguards**			
§164.310(a)	**Facility Access Controls**			
§164.310(a)(1)	Implement policies and procedures to limit physical access to [an entity's] electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	Facility Access Controls	Inspected and observed access policies and physical access restrictions and authentication controls.	HIPAA Compliant
§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.	Contingency Operations	Inspected the results of the annual system redundancy and disaster recovery testing.	HIPAA Compliant
§164.310(a)(2)(ii)	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	Facility Security Plan	Inspected and observed access policies and physical access restrictions and authentication controls based on user roles.	HIPAA Compliant

HIPAA Established Performance Criteria		Implementation Specification / Key Activity	Tests of Operating Effectiveness	Test Results
§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.	Access Control and Validation Procedures	Inspected and observed access policies and physical access restrictions and authentication controls based on user roles and visitors to the facilities.	HIPAA Compliant
§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).	Maintain Maintenance Records	Inspected a sample of monthly security reports which address identifying and repairing physical components of the security system.	HIPAA Compliant
§164.310(b)	**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.	Workstation Use	Inspected the inventory management system reports, inventory reporting functionality, access control groups, and account settings including password and lockout requirements.	HIPAA Compliant
§164.310(c)	**Workstation Security**			
§164.310(c)	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	Workstation Security	Inspected and observed user access listings and physical controls in place restricting access to company workstations and systems.	HIPAA Compliant

HIPAA Established Performance Criteria		Implementation Specification / Key Activity	Tests of Operating Effectiveness	Test Results
§164.310(d)	**Device and Media Controls**			
§164.310(d)(1)	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information, into and out of a facility, and the movement of these items within the facility.	Device and Media Controls	Inspected and observed the media destruction policies and procedures.	HIPAA Compliant
§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.	Disposal	Inspected and observed the media destruction policies and procedures.	HIPAA Compliant
§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.	Media Re-use	Inspected and observed the media destruction policies and procedures.	HIPAA Compliant
§164.310(d)(2)(iii)	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Accountability	Inspected and observed the media destruction policies and procedures.	HIPAA Compliant
§164.310(d)(2)(iv)	Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	Data Backup and Storage Procedures	This criteria is not applicable to Liquid Web as Liquid Web does not maintain ePHI for customers.	Not Applicable

HIPAA Established Performance Criteria		Implementation Specification / Key Activity	Tests of Operating Effectiveness	Test Results
§164.312	**Technical Safeguards**			
§164.312(a)	**Access Control**			
§164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Access Control	Inspected documentation for a sample of new hires, access modifications, terminations, and access reviews to ensure appropriate controls were in place for granting, modifying, reviewing, and removing access within the company. Inspected authentication systems and user access listings for privileged users to ensure access was appropriately restricted.	HIPAA Compliant
§164.312(a)(2)(i)	Assign a unique name and/or number for identifying and tracking user identity.	Unique User Identification	Inspected authentication procedures and user access listings noting unique user names were required.	HIPAA Compliant
§164.312(a)(2)(ii)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	Emergency Access Procedure	This criteria is not applicable to Liquid Web as Liquid Web does maintain or have access customer's ePHI.	Not Applicable
§164.312(a)(2)(iii)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Automatic Logoff	Inspected company policies and observed session configurations.	HIPAA Compliant
§164.312(c)	**Integrity**			
§164.312(c)(1)	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Integrity	This criteria is not applicable to Liquid Web as Liquid Web does not maintain or have access customer's ePHI.	Not Applicable
§164.312(c)(2)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	Mechanism to Authenticate ePHI	This criteria is not applicable to Liquid Web as Liquid Web does not maintain or have access customer's ePHI.	Not Applicable
§164.312(d)	**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.	Person or Entity Authentication	This criteria is not applicable to Liquid Web as Liquid Web does maintain or have access customer's ePHI. It is the customer's responsibility to authenticate access to ePHI in their environments.	Not Applicable

HIPAA Established Performance Criteria		Implementation Specification / Key Activity	Tests of Operating Effectiveness	Test Results
§164.312(e)	**Transmission Security**			
§164.312(e)(1)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	Transmission	This criteria is not applicable to Liquid Web. Although Liquid Web provides products to secure data transmissions, it is the responsibility of Liquid Web to implement and maintain transmission security controls.	Not Applicable
§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.	Integrity Controls	This criteria is not applicable to Liquid Web. Although Liquid Web provides products to secure data transmissions, it is the responsibility of Liquid Web to implement and maintain transmission security controls.	Not Applicable
§164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	Encryption	This criteria is not applicable to Liquid Web. Although Liquid Web provides products to secure data transmissions, it is the responsibility of Liquid Web to implement and maintain transmission security controls.	Not Applicable
§164.314	**Organizational Requirements**			
§164.314(a)	**Business Associate Contracts and Other Arrangements**			
164.314(a)(1)	The contract or other arrangement between the covered entity and its business associate required by § 164.308(b)(3) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable.	Business Associate Contracts or Other Arrangements	Liquid Web is not a covered entity and does not have business associates.	Not Applicable
164.314(a)(2)(i)(A)	The contract must provide that the business associate will— (A) Comply with the applicable requirements of this subpart;	Business associate contracts	Liquid Web is not a covered entity and does not have business associates.	Not Applicable

HIPAA Established Performance Criteria		Implementation Specification / Key Activity	Tests of Operating Effectiveness	Test Results
164.314(a)(2)(i)(B)	The contract must provide that the business associate will, in accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section.	Business associate contracts.	Liquid Web is not a covered entity and does not have business associates.	Not Applicable
164.314(a)(2)(i)(C)	The contract must provide that the business associate will report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.	Business associate contracts.	Liquid Web is not a covered entity and does not have business associates.	Not Applicable
164.314(a)(2)(ii)	The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).	Other Arrangements	Liquid Web is not a covered entity and does not have business associates.	Not Applicable
164.314(a)(2)(iii)	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.	Business associate contracts with subcontractors	Liquid Web is not a covered entity and does not have business associates.	Not Applicable

HIPAA Established Performance Criteria		Implementation Specification / Key Activity	Tests of Operating Effectiveness	Test Results
§164.316(a)	**Policies and Procedures**			
§164.316(a)	Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.	Policies and Procedures	Inspected the assigned responsibility for and company policies and procedures.	HIPAA Compliant
§164.316(a)	**Documentation**			
§164.316(b)(1)(i)	Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and	Documentation	Inspected the assigned responsibility for and company policies and procedures.	HIPAA Compliant
§164.316(b)(1)(ii)	If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record or the action, activity, or assessment.	Documentation	Inspected the policies and procedures related to maintenance of policies and evidence of the annual policy and procedure review and update process.	HIPAA Compliant
§164.316(b)(2)(i)	Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	Time Limit	Inspected evidence that the company policies and procedures on the company intranet.	HIPAA Compliant

HIPAA Established Performance Criteria		Implementation Specification / Key Activity	Tests of Operating Effectiveness	Test Results
§164.316(b)(2)(ii)	Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Availability	Inspected the policies and procedures on the company intranet and policy acknowledgement for a sample of new hires.	HIPAA Compliant
§164.316(b)(2)(iii)	Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	Updates	Inspected the policies and procedures related to maintenance of policies and evidence of the annual policy and procedure review and update process.	HIPAA Compliant