



LIGHTEGE SOLUTIONS, LLC

INDEPENDENT PRACTITIONER'S REPORT ON THE INFORMATION
SECURITY PROGRAM FOR THE COLOCATION, MANAGED, AND
HOSTED SERVICES SYSTEM RELATED TO HIPAA AND HITECH

JULY 31, 2022

Attestation and Compliance Services



Proprietary & Confidential

Reproduction or distribution in whole or in part without prior written consent is strictly prohibited.

This report is intended solely for use by the management of LightEdge Solutions, LLC, user entities of LightEdge Solutions, LLC's services, and other parties who have sufficient knowledge and understanding of LightEdge Solutions, LLC's services covered by this report (each referred to herein as a "specified user").

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

SECTION 1 INDEPENDENT PRACTITIONER'S REPORT	1
SECTION 2 MANAGEMENT'S ASSERTION	4
SECTION 3 DESCRIPTION OF THE INFORMATION SECURITY PROGRAM	6
SECTION 4 RESULTS	21

SECTION 1

INDEPENDENT PRACTITIONER'S REPORT

INDEPENDENT PRACTITIONER'S REPORT

To LightEdge Solutions, LLC:

Scope

We have examined LightEdge Solutions, LLC's ("LightEdge") management's assertion that the description of its information security program supporting the colocation, managed, and hosted services system that was provided to customer organizations (or "user entities") as of July 31, 2022, and included in Section 3 (the "description"), is fairly presented and that the information security program conforms, as of July 31, 2022, to the applicable implementation specifications within the Health Insurance Portability and Accountability Act ("HIPAA") Security Standards for the Protection of Electronic Protected Health Information ("HIPAA Security Rule") and the Notification in the Case of Breach of Unsecured Protected Health Information enacted as part of the American Recovery and Reinvestment Act of 2009 ("HITECH Breach Notification Requirements"), as described in Part 164 of CFR 45, in accordance with the criteria set forth in Section 2 ("management's assertion").

LightEdge uses a subservice organization for data center hosting services for one of the in-scope facilities. The description in Section 3 includes only the information security program of LightEdge and excludes the controls, procedures, and the information security at the subservice organization. Our examination did not extend to controls, procedures, and the information security program at the subservice organization.

LightEdge's Responsibilities

LightEdge has provided the attached assertion, in Section 2, about the fairness of the presentation of the description based on the description criteria. LightEdge is responsible for preparing the description and the assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services and related controls covered by the description; determining the applicability of the implementation specifications; and implementing the controls described therein for conformance of its information security program to meet the HIPAA Security Rule and HITECH Breach Notification criteria.

Independent Practitioner's Responsibilities

Our responsibility is to express an opinion 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 information security program supporting the colocation, managed, and hosted services system and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Inherent Limitations

Our organization is a licensed and independent CPA firm; however, our examination does not constitute a legal determination of compliance with the relevant regulations or a substitute for audit procedures that may be applied separately by regulatory entities. The specific procedures we performed, the nature, timing, and results of our tests are presented in Section 4 of our report titled "Results."

Because of their nature, controls may not prevent, or detect and correct, all errors or omissions relevant to the information security program. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the effectiveness of the information security program, is subject to the risk that controls may become inadequate or fail.

Opinion

In our opinion, based on the criteria described in LightEdge's assertion in Section 2, in all material respects,

- a. the description fairly presents the information security program supporting the colocation, managed, and hosted services system that was provided to user entities, as of July 31, 2022; and

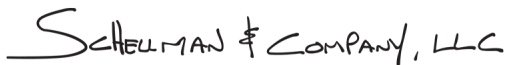
- b. the information security program conformed to the applicable implementation specifications within the HIPAA Security Rule and the HITECH Breach Notification Requirements, as described in Part 164 of CFR 45, as of July 31, 2022.

Restricted Use

This report, including the Results, is intended solely for the information and use of LightEdge and user entities of the colocation, managed, and hosted services system that was provided to user entities as of July 31, 2022, who have sufficient knowledge and understanding of the following:

- The nature of the service provided by LightEdge;
- The nature of the data provided to LightEdge and the definition of protected health information;
- How LightEdge's system interacts with user entities;
- Internal control and its limitations;
- The applicable HIPAA Security Rule and HITECH Breach Notification Requirements; and
- The risks that may threaten the achievement of the applicable HIPAA Security Rule and HITECH Breach Notification Requirements and how controls address those risks.

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

 SCHELMAN & COMPANY, LLC

Tampa, Florida
August 29, 2022

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the description of LightEdge Solutions, LLC's ("LightEdge") information security program supporting the colocation, managed, and hosted services system that was provided to customer organizations (or "user entities") as of July 31, 2022.

LightEdge uses a subservice organization for data center hosting services for one of the in-scope facilities. The description in Section 3 includes only the information security program of LightEdge and excludes the controls, procedures, and the information security program at the subservice organization.

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

- a. the description fairly presents the colocation, managed, and hosted services system made available to user entities of the system as of July 31, 2022. The criteria we used in making this assertion were that the description:
 - i. presents how the information security program was designed and implemented to govern the security policies and practices supporting the colocation, managed, and hosted services system;
 - ii. describes the relevant safeguards, standards, and rules deemed applicable by management;
 - iii. describes the specified controls within the information security program designed to achieve the information security program's objectives (the "Controls");
 - iv. does not omit or distort information relevant to the information security program, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system, and may not, therefore, include every aspect of the colocation, managed, and hosted services system that each individual user entity of the system and its auditor may consider important in its own particular environment; and
- b. The information security program supporting the colocation, managed, and hosted services system conforms, as of July 31, 2022, to the applicable implementation specifications within the Health Insurance Portability and Accountability Act ("HIPAA") Security Standards for the Protection of Electronic Protected Health Information ("HIPAA Security Rule") and the Notification in the Case of Breach of Unsecured Protected Health Information enacted as part of the American Recovery and Reinvestment Act of 2009 ("HITECH Breach Notification Requirements"), as described in Part 164 of CFR 45. The criteria we used in making this assertion were that:
 - i. management determined the applicable Controls included in the information security program;
 - ii. the Controls, as described, met implementation specifications for the applicable safeguards, standards, and rules, as defined in HIPAA Security Rule and HITECH Breach Notification Requirements; and
 - iii. the Controls, as described, were implemented as of July 31, 2022.

Section 3 of this report includes LightEdge's description of its colocation, managed, and hosted services system that is covered by this assertion.

SECTION 3

DESCRIPTION OF THE INFORMATION SECURITY PROGRAM

OVERVIEW OF OPERATIONS

Company Background

Founded in 1996, and headquartered in Des Moines, Iowa, LightEdge Solutions, LLC (“LightEdge” or the “Company”) provides an alternative for businesses that traditionally have purchased, maintained, and then depreciated equipment related to IT functions. By leveraging the economies of scale and LightEdge’s networking, cloud, colocation, and security expertise, customers are able to operate their applications and data on redundant IT platforms.

INFORMATION SECURITY PROGRAM

Description of Services Provided

LightEdge provides technology infrastructure for companies that require elevated levels of security and availability. LightEdge operates multiple enterprise-class data centers where they deploy hybrid solutions built on dedicated private cloud, managed hosting, and colocation services. LightEdge specializes in working with companies facing the most stringent regulatory requirements to help ensure compliance with industry standards.

The scope of the examination included LightEdge’s colocation, managed, and hosted services system at the following data center facilities:

Data Center	Facility Address
Altoona 1	1435 Northridge Circle, Altoona, Iowa 50009
Altoona 2	1401 Northridge Circle, Altoona, Iowa 50009
Austin 1	2916 Montopolis Drive, Suite 300, Austin, Texas 78741
Austin 2	7000-B Burleson Road, Suite 400, Austin, Texas 78744
Kansas City	9050 NE Underground Drive, Pillar 312, Kansas City, Missouri 64161
Omaha	1148 American Parkway, Papillion, Nebraska, 68046
Raleigh	8020 Arco Corporate Drive, Suite 310, Raleigh, North Carolina, 27617
Lenexa	17501 W 98 th Street, Lenexa, Kansas 66219
San Diego 1	9305 Lightwave Avenue, San Diego, California 92123
San Diego 2	9725 Scranton Road, San Diego, California 92121
Phoenix 1	120 East Van Buren, Phoenix, Arizona 85004

The aforementioned facilities are supported by personnel located at the Des Moines, Iowa, corporate office facility and on-site staff at each data center facility.

LightEdge keeps security and end-to-end customer care at the forefront of the services provided through the implementation of its service offerings and a 24x7x365 monitored Network Operations Center (NOC).

LightEdge offers a variety of IT services to its customers, which are further defined below:

Data Center Solutions

Colocation solutions in facilities specifically designed to meet customer requirements for computing and storage. Data center services can be customized for individual customer needs including:

- Rack Colocation
- Cage Space
- Private Suites
- Shared Colocation

Cloud Services

Hosted infrastructure solutions with scalable virtual, dedicated or hybrid solutions for servers, storage, and applications.

- Virtual Private Cloud
- Dedicated Private Cloud
- Bare Metal Cloud
- Power Cloud

Data Protection & Business Continuity Solutions

Backup and replication solutions customized for customer environments to ensure applications and data are protected.

- Managed Backup & Recovery
- Managed Data Protection
- Managed Disaster Recovery
- Workplace Recovery

Security Services

Enterprise-grade data center security solutions for mission-critical applications hosting sensitive data, including:

- Access Controls
- Private Network
- Load Balancing & Web Application Firewalling
- Next Generation Firewalling
- Security Information & Event Management (SIEM)
- Intrusion Detection & Prevention
- 24x7x365 Security Operations Center
- Vulnerability Management
- Data Encryption

Description of Electronic Protected Health Information (ePHI) Data Flows

LightEdge Solutions does not manage or access ePHI. Clients may manage ePHI within LightEdge's colocation, managed, and hosted services system.

Security Program Description

LightEdge has developed an information security management program to meet the information security and compliance requirements of the colocation, managed, and hosted services and its customer base. The program incorporates the elements of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule of 2003 and the Health Information Technology for Economic and Clinical Health (HITECH) Act. The description below is a summary of safeguards that LightEdge has implemented to adhere to the applicable components of the HIPAA Security Rule and the HITECH Breach Notification Requirements.

Documented information security policies are in place to govern acceptable use of information systems and to guide personnel in safeguarding systems infrastructure, information assets and data related to the colocation, managed, and hosted services. Information sensitivity classifications and employee guidelines are established for the handling and labeling of information based on sensitivity, value, and criticality. The policies and procedures address safeguards that LightEdge has implemented to adhere to the applicable components of the HIPAA Security Rule and the HITECH Breach Notification Requirements, and include multiple areas of security such as:

- Acceptable use
- Access control
- Capacity management
- Change management
- Configuration management
- Cryptographic controls and key management
- Disposal and destruction
- Employee handbook
- Incident and problem management
- Information classification, handling, and labeling of assets
- Information security
- LightEdge data center standard operating procedures
- Risk assessment and treatment
- Service design
- Service management system
- Vulnerability management

Policies are reviewed and approved by management on at least an annual basis. The review is performed by management personnel from various business functions, such as: Human Resources, Business Operations, Chief Security Officer, and Chief Operations Officer.

Security Awareness Training

Security policies are documented and available to employees on an internal web site. Employees receive security awareness training for information security as part of the onboarding process and on a monthly basis thereafter. An internal system is utilized to track and monitor completion of the training. This training is reinforced by security awareness newsletters and bulletins on current issues which are distributed periodically.

Periodic Testing and Evaluation

Management has implemented an internal audit program to evaluate the performance of specific control activities and processes over time and confirm that the in-scope controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority. The internal audit program assesses control activities that have been implemented to mitigate risks identified as part of the risk assessment process. Control activities within the scope are assigned a risk level associated with the assessed level of risk it is intended to mitigate; controls that serve to mitigate multiple risks are assigned the highest

level of assessed risk among the pertinent risks. Results of the internal audit process, including findings, are communicated to members of the Senior Management Team.

The Senior Management Team meets on a monthly basis to review company issues and plan direction. Reviews of current and upcoming audits (internal and external) are performed quarterly during these meetings and input is solicited from team members. Product Managers are encouraged to review controls impacting their products and provide feedback to further enhance compliance efforts.

Remediation and Continuous Improvement

Management has developed protocols to ensure findings of internal control deficiencies are reported to the individual responsible for taking corrective action for the function or activity involved and to at least one level of management above the directly responsible person. This process enables support and oversight of the corrective action as well as the communication with others in the organization whose activities may be affected. Deficiencies identified via the ongoing monitoring activities are further investigated by the Compliance and Security Team and members of the management team, as applicable. Deficiencies are tracked from identification to resolution. Customer complaints are received via a public e-mail address and reviewed on a quarterly basis for consideration on how to improve control activities. Regulator comments and feedback are incorporated and reviewed by Senior Management at the conclusion of any audit or auditable actions.

Incident Response

Documented incident response and support procedures are in place to guide operations personnel in the monitoring, documenting, escalating, and resolving of problems affecting colocation, managed, and hosted services. These procedures include severity level definitions, escalation, ticket handling, and response time requirements for service alerts. Operations personnel utilize a centralized ticketing system to document, prioritize, escalate, and resolve problems affecting contracted services. Additionally, key performance indicator (KPI) reports are generated by the online operational metrics reporting dashboard and reviewed by management during the monthly management meetings to evaluate system incident, response, and resolution activities.

LightEdge provides a web portal for customers to perform basic administration and performance monitoring of services purchased by those customers. Customers are able to retrieve performance logs on a circuit-by-circuit basis and are able to open trouble tickets for incidents or requests related to the services in which they are enrolled.

Centralized ticketing systems are used to track customer support requests and incidents as well as change requests for production systems. Reports can be generated from the ticketing and request systems for trending and analysis.

Third-Party Services and Monitoring

No subservice organizations were included in the scope of this assessment, including the data center hosting services provided by Digital Realty at the Phoenix 1 data center. As noted in Section 4, Digital Realty is responsible for the physical and environmental controls and associated safeguards at the Phoenix 1 data center.

LightEdge performs periodic reviews of audit reports to help ensure continual compliance by vendors and business partners. Vendors that help to support the in-scope services are assessed on an annual basis which includes an assessment of audit reports or completion of a security assessment.

Breach Notification Description

Breach Notification Policies and Procedures

Documented breach notification policies and procedures are in place to guide personnel in the identification of a breach, including the following: defining the circumstance where a breach shall be deemed to have occurred, the timing and required information to be included in a notification, required workforce training, and the required action if a law enforcement officials state that a notification would impede a criminal investigation. The legal counsel will comply with any law enforcement related requests in relation to breach notification. The breach notification policy is reviewed at least annually and updated, as necessary.

Incident Reporting Process

Security incidents are reported to management are documented and tracked within a data breach and investigation incident report, which contains the steps followed to resolve the incident. The security incident report also includes a summary of the incident, host(s) and system(s) affected, an incident assessment to elaborate the damage resulting from the incident, and the resolution performed to remediate. LightEdge also performs a test of their incident response plan on an annual basis.

Notification Requirements

Documented breach notification policies and procedures are in place that define the required content of the breach notification. Employees are required complete training upon hire and on an annual basis thereafter to understand their obligations and responsibilities as it relates to HIPAA breach notification requirements. Policies and procedures also exist to help guide personnel and address the following areas: assessment, breach exception, and notification to affected parties. If it is determined that breach notification is required, senior management personnel follow designated steps to provide written notice to relevant parties within 30 days unless otherwise stated by law. These steps include coordinating with designated counsel to determine required notifications.

Risk Assessments

Risk assessments are performed on at least an annual basis according to the risk assessment and treatment policy to identify risks that could result in impermissible acquisition, access, use, or disclosure of PHI. Additionally, assessments are performed on identified security incidents to determine if impermissible acquisition, access, use, or disclosure of PHI occurred.

RISK ASSESSMENT

Risk Assessment Scoping

LightEdge recognizes the importance of the ongoing identification and management of risk in order to provide management reasonable assurance that LightEdge's strategic and operational objectives can be achieved. The risk assessment process includes identification and analysis of risks that pose a threat the organization's ability to perform the in-scope services. The process starts with determining the organization's objectives as these objectives are key to understanding the risks and allows identification and analysis of those risks relative to the objectives. Management has committed to customers to carry out certain objectives in relation to the services provided. These commitments are documented to ensure that the operations, reporting, and compliance objectives are aligned with the commitments and company's mission.

LightEdge has considered risks that could affect the organization's ability to provide reliable colocation, managed, and hosted services to its user entities. Management considers risks that could affect customers based on the services to which they subscribe, for example:

- Risks for network customers include loss of service due to misconfiguration, upstream outages, or physical disruption. For managed security services, risks include misconfiguration, flaws in code running on the firewalls, and traffic overflows. Risks for backup customers include misconfiguration or failure of equipment.
- Risks related to software errors are handled by subscribing to and reviewing error report lists from major manufacturers. Applicable systems are upgraded when a significant security flaw is identified to the latest generally stable release of code.
- Risks for colocation customers are failure of electric delivery or cooling systems. Physical issues are addressed with daily systems reviews, preventative maintenance, and automated monitoring.

The LightEdge risk assessment process focuses on supporting management decisions and responding to potential threats by assessing risks and identifying important decision factors. Identification and resolution of longer-term issues are left to the project management teams and are handled as defined projects for completion by each team.

Potential Threats, Vulnerabilities and Current Security Measures

Management considers risks that can arise from both external and internal factors including the following:

External Factors

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes, or personnel
- Types of fraud, including fraud incentives and pressures for employees, fraud opportunities, and employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities

Threat and Vulnerability Identification

LightEdge performs ongoing monitoring to help ensure that business systems operate effectively as part of daily operations. Aspects of the ongoing monitoring procedures include the following:

- Logging and monitoring software is configured to collect data from in-scope systems and alert IT personnel upon detection of unusual activity.
- A monitoring application is in place to monitor the performance and availability of production sites, servers, and devices.
- An intrusion prevention system (IPS) is utilized to analyze and report network events and block suspected or actual network security breaches.
- Vulnerability assessments and penetration testing are performed on a monthly and annual basis, respectfully, to identify threats and assess their potential impact to system security and availability. Identified security vulnerabilities are triaged by the information security team and monitored through resolution.

Monitoring systems at LightEdge are set with automatic alerting thresholds that generate system alerts to the network operations team for any failures noted within LightEdge's systems. System alerts are categorized by severity and dispatched accordingly to operations teams for investigation. Automated alert and escalation processes are in place depending on severity level of an alert with Class 1 and Class 2 alerts receiving director of support and / or vice president level notification within four hours of occurrence, if not resolved.

Current Security Measures

LightEdge has developed an enterprise-wide information security management program to meet the information security and compliance requirements of LightEdge and its customer base. The program incorporates the elements of the Health Insurance Portability and Accountability Act Security Rule of 2003 (HIPAA Security Rule) and the HITECH Breach Notification Requirements.

The description below is a summary of safeguards that LightEdge has implemented to adhere to the applicable components of the HIPAA Security Rule and the Breach Notification Requirements of HITECH.

Administrative Safeguards

- *Security Management Process.* The organization implements policies and procedures to prevent, detect, contain, and correct security violations.
- *Risk Analysis.* The organization performs 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 Management.* The organization implements security measures sufficient to reduce risks and vulnerabilities to a reasonable level.
- *Sanction Policy.* The organization implements sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
- *Information Security Activity Review.* The organization implements procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
- *Assigned Security Responsibility.* The organization designates a 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.
- *Workforce Security.* The organization implements policies and procedures to ensure that members of its workforce have 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.
- *Authorization and/or Supervision.* The organization implements 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.
- *Workforce Clearance Procedure.* The organization implements procedures to determine that the access of a workforce member to electronic protected health information is authorized.
- *Termination Procedures.* The organization implements 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) of this section.
- *Information Access Management.* The organization implements policies and procedures for authorizing access to electronic protected health information within the colocation, managed, and hosted environment only when such access is authorized based on the user or recipient's role (role-based access).
- *Access Authorization.* The organization implements 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 Establishment and Modification.* The organization implements 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.
- *Security Awareness and Training.* The organization implements a security awareness and training program for members of its workforce (including management).
- *Security Reminders.* The organization monitors periodic security updates.
- *Protection from Malicious Software.* The organization implements procedures for guarding against, detecting, and reporting malicious software.
- *Log-in Monitoring.* The organization implements procedures for monitoring log-in attempts and reporting discrepancies.
- *Password Management.* The organization implements procedures for creating, changing, and safeguarding passwords.
- *Security Incident Procedures.* The organization implements policies and procedures to address security incidents.

- *Response and Reporting.* Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.
- *Contingency Planning.* The organization establishes (and implements as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.
- *Data Backup Plan.* The organization establishes and implements and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
- *Disaster Recovery Plan.* Establish (and implement as needed) procedures to restore any loss of data.
- *Emergency Mode Operation Plan.* The organization establishes (and implements 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.
- *Testing and Revisions Procedures.* The organization implements procedures for periodic testing and revision of contingency plans.
- *Applications and Data Criticality Analysis.* Assess the relative criticality of specific applications and data in support of other contingency plan components.
- *Evaluation.* The organization performs a periodic technical and nontechnical evaluation, based initially upon the standards implemented under the HIPAA Security Rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of the HIPAA Security Rule.
- *Written Contract or Other Arrangement.* The organization documents 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 organizational requirements.

Physical Safeguards

- *Facility Access and Control.* The organization implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
- *Contingency Operations.* The organization establishes (and implements as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
- *Facility Security Plan.* The organization implements policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
- *Access Control and Validation Procedures.* The organization implements 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.
- *Maintenance Records.* The organization implements 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).
- *Workstation Use.* The organization implements 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 Security.* The organization implements physical safeguards for workstations that access electronic protected health information, to restrict access to authorized users.

- *Device and Media Controls.* The organization implements 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.
- *Disposal.* The organization implements 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.
- *Media Re-use.* The organization implements procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.
- *Accountability.* The organization maintains a record of the movements of hardware and electronic media and responsible persons.
- *Data backup and storage.* The organization creates a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Technical Safeguards

- *Access Control.* The organization implements 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 administrative requirements.
- *Unique User Identification.* The organization assigns a unique name and/or number for identifying and tracking user identity.
- *Emergency Access Procedure.* The organization establishes (and implements as needed) procedures for obtaining necessary electronic protected health information during an emergency.
- *Automatic log-off.* The organization implements electronic procedures that terminate an electronic session after a predetermined time of inactivity.
- *Encryption and Decryption.* Implement a mechanism to encrypt and decrypt electronic protected health information.
- *Audit Controls.* The organization implements hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
- *Integrity.* The organization implements policies and procedures to protect electronic protected health information from improper alteration or destruction.
- *Mechanism to authenticate electronic protected health information.* The organization implements electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.
- *Person or entity authentication.* The organization implements procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
- *Transmission Security.* The organization implements technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
- *Integrity controls.* The organization implements security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.
- *Encryption.* The organization implements a mechanism to encrypt electronic protected health information.

Breach Notification

- *General Rule.* The business associate, following the discovery of a breach of unsecured protected health information, provides a notification to the covered entity of such breach.
- *Breaches Treated as Discovered.* A breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been

known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency).

- *Timeliness of Notification.* The business associate provides a notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
- *Content of Notification.*
 - The business associate provides a notification that shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.
 - The business associate provides the covered entity with any other available information that the covered entity is required to include in notification to the individual under §164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.
- *Burden of Proof.* The business associate shall have the burden of demonstrating that notifications were made in the event of a use or disclosure in violation.

Likelihood / Impact Analysis

Likelihood of Threat Occurrence and Impact Analysis

Risk analysis is an essential process to LightEdge's continued success. Senior Management has implemented a process whereby the likelihood and consequence of various risks to the in-scope services have been assessed. Senior leadership broadly defines risk levels to the identified risks, according to the following three categories: low risk, moderate risk, and high risk. A formal risk assessment is performed on an annual basis; however, risks are identified on an ongoing basis and assessed by the Compliance and Security Team.

Risk Level Determination / Documentation

Risk treatment is recorded in the risk register. Risks with a low score are treated as accepted in the risk register and marked as such. Risks with a medium or high score remain open until treated, transferred to a third party, avoided, or accepted. One or more treatment options must be selected for risks with a medium or high score:

- Selection of security control(s) from Annex A of the ISO/IEC 27001 standard or another standard such as the controls defined within the System and Organization Controls (SOC) 1 or SOC 2 reports
- Transferring the risk to a third party – examples include purchasing an insurance policy or signing a contract with suppliers or partners
- Avoiding the risk by discontinuing a business activity that causes such risk
- Accepting the risk – this option is allowed only if the selection of other risk treatment options would cost more than the potential impact should such risk materialize

Identified risks are reviewed regularly to ensure effectiveness of the Risk Management Policy. The review is conducted during the quarterly management review meetings, or more frequently in the case of significant organizational changes, significant change in technology, change of business objectives, changes in the business environment, etc.

LightEdge operates a peer reviewed change management process to help ensure that network and system level changes are fully reviewed and understood prior to implementation, thus reducing the risk of additional vulnerabilities being introduced into the production environment.

The chief security officer documents the following in the Statement of Applicability (SOA):

- Justification for inclusion or exclusion of controls
- Control implementation status

Senior Management accepts residual risks through the SOA and the chief security officer will prepare the risk treatment plan within the SOA in which the implementation of controls will be planned. Senior Management approves the risk treatment plan during the quarterly management review meetings.

Risk Management Program Monitoring and Maintenance

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control objectives have been defined for each significant risk area. Control activities are then defined to serve as mechanisms for managing the achievement of those objectives and help ensure that the actions associated with those risks are carried out properly and efficiently.

Management has implemented an internal audit program to evaluate the performance of specific control activities and processes over time and confirm that the in-scope controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority. The internal audit program assesses control activities that have been implemented to mitigate risks identified as part of the risk assessment process. Control activities within the scope are assigned a risk level associated with the assessed level of risk it is intended to mitigate; controls that serve to mitigate multiple risks are assigned the highest level of assessed risk among the pertinent risks. Results of the internal audit process, including findings, are communicated to members of the Senior Management Team.

APPLICABLE SAFEGUARDS

LightEdge, in providing the colocation and managed services, is considered a business associate. LightEdge does not work under a covered entity’s workforce but still would have access to ePHI, should ePHI be in the colocation, managed, and hosted services. Business associates, like covered entities, have the responsibility to achieve and maintain HIPAA compliance.

LightEdge management has made the determination regarding the applicability of the established performance criteria as it pertains to the in-scope services (the “applicable safeguards”).

The table below provides the regulation references (section) and key activity, which relate to the established performance criteria, that LightEdge management has asserted to be in-scope for the purposes of this attestation:

Section	Key Activity	Applicable Safeguards	
		Yes	No
<u>Security</u>			
§164.306(a)	General Requirements	P	
§164.306(b)	Flexibility of Approach	P	
§164.308(a)	Security Management Process	P	
§164.308(a)(1)(ii)(A)	Security Management Process – Risk Analysis	P	
§164.308(a)(1)(ii)(B)	Security Management Process – Risk Management	P	
§164.308(a)(1)(ii)(C)	Security Management Process – Sanction Policy	P	
§164.308(a)(1)(ii)(D)	Security Management Process – Information System Activity Review	P	
§164.308(a)(2)	Assigned Security Responsibility	P	
§164.308(a)(3)(i)	Workforce Security	P	

Section	Key Activity	Applicable Safeguards	
		Yes	No
§164.308(a)(3)(ii)(A)	Workforce Security – Authorization and/or Supervision	P	
§164.308(a)(3)(ii)(B)	Workforce Security – Workforce Clearance Procedure	P	
§164.308(a)(3)(ii)(C)	Workforce Security – Establish Termination Procedures	P	
§164.308(a)(4)(i)	Information Access Management	P	
§164.308(a)(4)(ii)(A)	Information Access Management – Isolating Healthcare Clearinghouse Functions		P
§164.308(a)(4)(ii)(B)	Information Access Management – Access Authorization	P	
§164.308(a)(4)(ii)(C)	Information Access Management – Access Establishment and Modification	P	
§164.308(a)(5)(i)	Security Awareness and Training	P	
§164.308(a)(5)(ii)(A)	Security Awareness and Training – Security Reminders	P	
§164.308(a)(5)(ii)(B)	Security Awareness, Training, and Tools – Protection from Malicious Software	P	
§164.308(a)(5)(ii)(C)	Security Awareness, Training, and Tools – Log-in Monitoring	P	
§164.308(a)(5)(ii)(D)	Security Awareness, Training, and Tools – Password Management	P	
§164.308(a)(6)(i)	Security Incident Procedures	P	
§164.308(a)(6)(ii)	Security Incident Procedures – Response and Reporting	P	
§164.308(a)(7)(i)	Contingency Plan	P	
§164.308(a)(7)(ii)(A)	Contingency Plan – Data Backup Plan	P	
§164.308(a)(7)(ii)(B)	Contingency Plan – Disaster Recovery Plan	P	
§164.308(a)(7)(ii)(C)	Contingency Plan – Emergency Mode Operation Plan	P	
§164.308(a)(7)(ii)(D)	Contingency Plan – Testing and Revision Procedure	P	
§164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis	P	
§164.308(a)(8)	Evaluation of Analysis	P	
§164.308(b)(1)	Business Associate Contracts and Other Arrangements		P
§164.308(b)(2)	Assigned Security Responsibility		P
§164.308(b)(3)	Business Associate Contracts and Other Arrangements – Written Contract or Other Arrangement		P
§164.310(a)(1)	Facility Access Controls	P	
§164.310(a)(2)(i)	Facility Access Controls – Contingency Operations	P	

Section	Key Activity	Applicable Safeguards	
		Yes	No
§164.310(a)(2)(ii)	Facility Access Controls – Facility Security Plan	P	
§164.310(a)(2)(iii)	Facility Access Controls – Access Control and Validation Procedures	P	
§164.310(a)(2)(iv)	Facility Access Controls – Maintain Maintenance Records	P	
§164.310(b)	Workstation Use	P	
§164.310(c)	Workstation Security	P	
§164.310(d)(1)	Device and Media Controls	P	
§164.310(d)(2)(i)	Device and Media Controls – Disposal	P	
§164.310(d)(2)(ii)	Device and Media Controls – Media Re-use	P	
§164.310(d)(2)(iii)	Device and Media Controls – Accountability	P	
§164.310(d)(2)(iv)	Device and Media Controls – Data Backup and Storage Procedures	P	
§164.312(a)(1)	Access Control	P	
§164.312(a)(2)(i)	Access Control – Unique User Identification	P	
§164.312(a)(2)(ii)	Access Control – Emergency Access Procedure	P	
§164.312(a)(2)(iii)	Access Control – Automatic Logoff	P	
§164.312(a)(2)(iv)	Access Control – Encryption and Decryption	P	
§164.312(b)	Audit Controls	P	
§164.312(c)(1)	Integrity	P	
§164.312(c)(2)	Integrity – Mechanism to Authenticate ePHI	P	
§164.312(d)	Person or Entity Authentication	P	
§164.312(e)(1)	Transmission	P	
§164.312(e)(2)(i)	Transmission Security – Integrity Controls	P	
§164.312(e)(2)(ii)	Transmission Security – Encryption	P	
§164.314(a)(1)	Business Associate Contracts or Other Arrangements		P
§164.314(a)(2)(i)(A)	Business Associate Contracts		P
§164.314(a)(2)(i)(B)	Business Associate Contracts		P
§164.314(a)(2)(i)(C)	Business Associate Contracts		P
§164.314(a)(2)(ii)	Other Arrangements		P
§164.314(a)(2)(iii)	Business Associate Contracts with Subcontractors		P
§164.314(a)(b)(1)	Requirements for Group Health Plans		P
§164.314(b)(2)(i)	Group Health Plan Implementation Specification		P
§164.314(b)(2)(ii)	Group Health Plan Implementation Specification		P
§164.314(b)(2)(iii)	Group Health Plan Implementation Specification		P
§164.314(b)(2)(iv)	Group Health Plan Implementation Specification		P

Section	Key Activity	Applicable Safeguards	
		Yes	No
§164.316(a)	Policies and Procedures	P	
§164.316(b)(1)	Documentation	P	
§164.316(b)(2)(i)	Documentation	P	
§164.316(b)(2)(ii)	Documentation	P	
§164.316(b)(2)(iii)	Documentation	P	
<u>Breach Notification</u>			
§164.414(a)	Administrative Requirements		P
§164.530(b)	Training	P	
§164.530(d)	Complaints		P
§164.530(e)	Sanctions		P
§164.530(g)	Refraining from Retaliatory Acts		P
§164.530(h)	Waiver of Rights		P
§164.530(i)	Policies and Procedures		P
§164.530(j)	Documentation		P
§164.402	Definitions: Breach – Risk Assessment, Breach Exceptions - Unsecured PHI	P	
§164.404(a)(1)	Notice to Individuals		P
§164.404(b)	Timeliness of Notification		P
§164.404(c)(1)	Content of Notification		P
§164.404(d)	Methods of Notification		P
§164.406	Notification to the Media		P
§164.408	Notification to the Secretary		P
§164.410	Notification by a Business Associate	P	
§164.412	Law Enforcement Delay	P	
§164.414(b)	Burden of Proof	P	

The specific established performance criteria are detailed in Section 4 (“Results”) of this report.

Section 4 also provides the results related to the security and breach performance criteria as selected from the applicability table above.

SECTION 4

RESULTS

HIPAA SECURITY RULE

#	Control Activity Specified by the Service Organization	Results
<p>§164.306(a): Covered entities and business associates must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part; and (4) Ensure compliance with this subpart by its workforce.</p>		
1.01	Documented security policies and procedures are in place to guide personnel in practices and principles related to the HIPAA Security Rule.	Control implemented.
<p>§164.306(b): Flexibility of approach. (1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. (2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors: (i) The size, complexity, and capabilities of the covered entity or business associate. (ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities. (iii) The costs of security measures. (iv) The probability and criticality of potential risks to electronic protected health information.</p>		
1.02	Documented security policies and procedures are in place to guide personnel in practices and principles related to the HIPAA Security Rule.	Control implemented.
1.03	<p>A formal risk assessment is performed on at least an annual basis to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. Risks that are identified are rated using a risk evaluation process and are formally documented that includes the following factors:</p> <ul style="list-style-type: none"> • Size, complexity, and capabilities • Technical infrastructure, hardware, and software security capabilities • Costs of security measures • Probability and criticality of potential risks to ePHI 	Control implemented.
1.04	A ticketing system is utilized to document, track, and resolve reported security violations.	Control implemented.
<p>§164.308(a): A covered entity or business associate must in accordance with §164.306: (1)(i) Implement policies and procedures to prevent, detect, contain, and correct security violations.</p>		
1.05	Documented security policies and procedures are in place to guide personnel in the prevention, detection, containment, and correction of security violations.	Control implemented.
1.06	Documented security policies and procedures are communicated to employees via the company intranet.	Control implemented.
1.07	Employees complete security awareness training upon hire, and annually thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Control implemented.
1.08	A ticketing system is utilized to document, track, and resolve reported security violations.	Control implemented.
<p>§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.</p>		
1.09	Documented policies and procedures are in place to guide personnel in the assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.	Control implemented.

#	Control Activity Specified by the Service Organization	Results
1.10	A formal risk assessment is performed on at least an annual basis to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. Risks that are identified are rated using a risk evaluation process and are formally documented that includes the following factors: <ul style="list-style-type: none"> Size, complexity, and capabilities Technical infrastructure, hardware, and software security capabilities Costs of security measures Probability and criticality of potential risks to ePHI 	Control implemented.
§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).		
1.11	Documented policies and procedures are in place to guide personnel in the risk management process to reduce risks and vulnerabilities to a reasonable and appropriate level.	Control implemented.
1.12	Risks that are identified in the risk assessment are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Control implemented.
1.13	Employees sign an acknowledgment form upon hire, indicating that they have been given access to the employee manual and electronic communications policy and understand their responsibility for adhering to the code of conduct outlined within the manual.	Control implemented.
1.14	Newly hired employees sign a written acknowledgment form documenting their receipt and understanding of the requirement to protect confidential information.	Control implemented.
1.15	Employees complete security awareness training upon hire, and annually thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Control implemented.
§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.		
1.16	Documented sanction policies and procedures are in place for action to be taken when workforce members fail to comply with the security policies and procedures.	Control implemented.
1.17	Employees sign an acknowledgment form upon hire, indicating that they have been given access to the employee manual and electronic communications policy and understand their responsibility for adhering to the code of conduct outlined within the manual.	Control implemented.
1.18	Sanctions are applied to workforce members when violations of the security policies and procedures are discovered.	Control implemented.
§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.		
1.19	Documented system logging and auditing policies and procedures are in place to guide personnel in the review of records of information system activities.	Control implemented.
1.20	Logging and monitoring software is configured to collect data from in-scope systems and alert IT personnel upon detection of unusual activity.	Control implemented.
§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.		
1.21	Responsibility of the development and implementation of information security policies and procedures is formally assigned to the chief security officer and the responsibilities of the Security Official have been defined.	Control implemented.

#	Control Activity Specified by the Service Organization	Results
§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.		
1.22	Documented policies and procedures are in place to guide personnel regarding access provisioning, modification, removal, and review.	Control implemented.
1.23	Access requests are documented on a standard access request form.	Control implemented.
1.24	Managers review user access to the in-scope systems containing ePHI on at least an annual basis to help ensure that access correlates with employee job functions and duties.	Control implemented.
1.25	Access to systems that host ePHI is restricted to appropriate personnel.	Control implemented.
§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.		
1.26	Documented policies and procedures are in place to guide personnel regarding access provisioning, modification, removal, and review.	Control implemented.
1.27	Managers approve user access requests for systems containing ePHI as documented on a standard access request form.	Control implemented.
1.28	Managers review user access to the in-scope systems containing ePHI on at least an annual basis to help ensure that access correlates with employee job functions and duties.	Control implemented.
1.29	Access to systems that host ePHI is restricted to appropriate personnel.	Control implemented.
1.30	Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of systems containing ePHI. These charts are communicated to employees and updated as needed.	Control implemented.
§164.308(a)(3)(ii)(B): Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.		
1.31	Documented policies and procedures are in place to guide personnel regarding access provisioning, modification, removal, and review.	Control implemented.
1.32	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Control implemented.
1.33	Managers approve user access requests for systems containing ePHI as documented on a standard access request form.	Control implemented.
1.34	Managers review user access to the in-scope systems containing ePHI on at least an annual basis to help ensure that access correlates with employee job functions and duties.	Control implemented.
1.35	Documented physical security policies and procedures are in place to guide personnel in physical security practices for secure areas.	Control implemented.
1.36	Background checks are performed for employees as a component of the hiring process.	Control implemented.
1.37	System owners revoke terminated employees' access to the in-scope systems as a component of the termination process.	Control implemented.
§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).		
1.38	Documented policies and procedures are in place to guide personnel regarding access provisioning, modification, removal, and review.	Control implemented.
1.39	System owners revoke terminated employees' access to the in-scope systems as a component of the termination process.	Control implemented.

#	Control Activity Specified by the Service Organization	Results
1.40	Access modification requests are documented on a standard access request form.	Control implemented.
§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.		
1.41	Documented policies and procedures are in place to guide personnel regarding access provisioning, modification, removal, and review.	Control implemented.
1.42	Access requests are documented on a standard access request form.	Control implemented.
1.43	Managers approve user access requests for systems containing ePHI as documented on a standard access request form.	Control implemented.
§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.		
Not applicable. LightEdge is not a health care clearinghouse.		
§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.		
1.44	Access requests are documented on a standard access request form.	Control implemented.
1.45	The in-scope systems are configured to authenticate users with a unique user account and enforce predefined user account and minimum password requirements.	Control implemented.
1.46	Documented policies and procedures are in place to guide personnel regarding access provisioning, modification, removal, and review.	Control implemented.
1.47	Access to systems that host ePHI is restricted to appropriate personnel.	Control implemented.
§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.		
1.48	Access requests are documented on a standard access request form.	Control implemented.
1.49	The in-scope systems are configured to authenticate users with a unique user account and enforce predefined user account and minimum password requirements.	Control implemented.
1.50	Documented policies and procedures are in place to guide personnel regarding access provisioning, modification, removal, and review.	Control implemented.
1.51	Access modification requests are documented on a standard access request form.	Control implemented.
1.52	Managers review user access to the in-scope systems containing ePHI on at least an annual basis to help ensure that access correlates with employee job functions and duties.	Control implemented.
§164.308(a)(5)(i): Implement a security awareness and training program for all members of its workforce (including management).		
1.53	<p>Policies and procedures regarding security awareness training are in place with elements that include the following:</p> <ul style="list-style-type: none"> • How workforce members are provided the security awareness and training • Identifies workforce members (including managers, senior executives, and as appropriate, business associates, and contractors) who will be provided with the security and awareness training • How workforce members will be provided with security and awareness training when there is a change in the entity's information systems • How frequently security awareness and training will be provided to all workforce members 	Control implemented.

#	Control Activity Specified by the Service Organization	Results
1.54	A formal security awareness training program is in place.	Control implemented.
1.55	Employees complete security awareness training upon hire, and annually thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Control implemented.
§164.308(a)(5)(ii)(A): Periodic security updates.		
1.56	The IT security group monitors the security impact of emerging technologies, and the impact of applicable laws or regulations are considered by senior management.	Control implemented.
1.57	Employees complete security awareness training upon hire, and annually thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Control implemented.
1.58	Security reminders and updates are communicated to workforce members on an ongoing basis.	Control implemented.
§164.308(a)(5)(ii)(B): Procedures for guarding against, detecting, and reporting malicious software.		
1.59	Documented network security policies and procedures are in place to help ensure that monitoring and prevention solutions are in place and that systems are maintained and monitored by personnel in accordance with predefined processes.	Control implemented.
1.60	Firewall systems are in place to filter unauthorized inbound network traffic from the Internet.	Control implemented.
1.61	The firewall systems are configured to deny any type of network connection that is not explicitly authorized by a firewall rule.	Control implemented.
1.62	The firewall systems are configured to provide failover firewall services in the event of a firewall system failure.	Control implemented.
1.63	The firewall systems are configured to log activity that includes the following: <ul style="list-style-type: none"> • Account logon events • Source address • Destination address 	Control implemented.
1.64	A central antivirus server is utilized to protect registered production Windows servers and workstations with the following configurations: <ul style="list-style-type: none"> • Scan for updates to antivirus definitions and update registered clients on a real-time basis • Scan registered clients on a daily basis 	Control implemented.
1.65	An IPS is utilized to analyze and report network events and block suspected or actual network security breaches.	Control implemented.
1.66	Operations personnel are sent alert notifications when certain network security events are detected.	Control implemented.
1.67	A ticketing system is utilized to manage system incidents, response, and resolution.	Control implemented.
1.68	Internal vulnerability scans are performed on a monthly basis to identify potential infrastructure security vulnerabilities.	Control implemented.
1.69	An independent penetration test specialist performs a network penetration assessment of the production infrastructure on an annual basis to identify potential security vulnerabilities.	Control implemented.
§164.308(a)(5)(ii)(C): Procedures for monitoring log-in attempts and reporting discrepancies.		
1.70	Documented system logging and auditing policies and procedures are in place to guide personnel in the review of records of information system activities.	Control implemented.

#	Control Activity Specified by the Service Organization	Results
1.71	<p>The in-scope systems are configured to log access related events including the following:</p> <ul style="list-style-type: none"> • Account management • Logon events • Object access • Policy change • Privileged use 	Control implemented.
1.72	The in-scope systems are configured to automatically notify operations personnel in the event that an event triggers a predefined alert.	Control implemented.
1.73	A ticketing system is utilized to manage system incidents, response, and resolution.	Control implemented.
§164.308(a)(5)(ii)(D): Procedures for creating, changing, and safeguarding passwords.		
1.74	A documented password policy is in place.	Control implemented.
1.75	The in-scope systems are configured to authenticate users with a unique user account and enforce predefined user account and minimum password requirements.	Control implemented.
1.76	Employees upon hire and on an annual basis thereafter complete training to understand their obligations and responsibilities to comply with the policies and procedures of protected health information, which includes creating, changing, and safeguarding passwords.	Control implemented.
§164.308(a)(6)(i): Implement policies and procedures to address security incidents.		
1.77	<p>Documented escalation procedures are in place to guide employees in the security incident response process that includes the following elements:</p> <ul style="list-style-type: none"> • Identification of what specific event would be considered a security incident • Identification of workforce members' role and responsibilities regarding security incidents • Management involvement regarding security incidents • Workforce members or roles to which the incident response policies and procedures are to be disseminated • Coordination of security incidents among business associates • Identifies what steps should be taken in response to a security incident • The frequency to review and update current security incident policies and procedures 	Control implemented.
1.78	A ticketing system is utilized to manage system incidents, response, and resolution.	Control implemented.
§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.		
1.79	<p>Documented incident response procedures are in place to guide personnel that includes the following:</p> <ul style="list-style-type: none"> • A methodology for defining security incidents based on levels of criticality • Provisions for reporting and responding to all types of known and suspicious security incidents based on criticality levels of such incidents • The roles and responsibilities of workforce members including the entity's security incident response team 	Control implemented.
1.80	A ticketing system is utilized to manage system incidents, response, and resolution.	Control implemented.

#	Control Activity Specified by the Service Organization	Results
§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.		
1.81	<p>A business continuity plan (BCP) / disaster recovery plan (DRP) is in place to guide personnel in procedures to protect against disruptions caused by an unexpected event that includes the following:</p> <ul style="list-style-type: none"> • Identification of workforce members' roles and responsibilities in the contingency process • Workforce members or roles to which the contingency policies and procedures are to be disseminated • Management involvement in contingency plans Coordination of contingency processes among business associates • Identification of what steps should be taken in a contingency plan • The frequency to review and update current contingency policies and procedures • How frequently the contingency plan is tested 	Control implemented.
1.82	Documented escalation procedures are in place to guide employees in reporting, acting upon, and resolving reported events.	Control implemented.
§164.308(a)(7)(ii)(A): Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.		
1.83	Documented backup policies and procedures are in place.	Control implemented.
1.84	An automated backup system is in place to perform scheduled backups of production servers on a weekly basis.	Control implemented.
1.85	An automated backup system is configured to perform backups of production data to disk on a daily basis.	Control implemented.
1.86	The backup system is configured to automatically replicate backup data to a geographically separate location on a daily basis.	Control implemented.
1.87	IT personnel perform restoration of backup files at least annually as a component of business operations to help ensure system recovery.	Control implemented.
§164.308(a)(7)(ii)(B): Establish (and implement as needed) procedures to restore any loss of data.		
1.88	A BCP/DRP is in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Control implemented.
1.89	IT personnel perform restoration of backup files at least annually as a component of business operations to help ensure system recovery.	Control implemented.
1.90	<p>Documented policies and procedures regarding data restoration are in place that includes the following:</p> <ul style="list-style-type: none"> • Workforce members' roles and responsibilities in the process of restoring lost data • Determination of what data will be restored • Identification of occurring events (e.g., disruption, compromise, failure) that require data restoration • Timeframe of data restoration • How frequently data restorations will be tested or assessed for verification of media reliability and data integrity 	Control implemented.
§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.		
1.91	A BCP/DRP is in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Control implemented.

#	Control Activity Specified by the Service Organization	Results
§164.308(a)(7)(ii)(D): Implement procedures for periodic testing and revision of contingency plans.		
1.92	<p>Documented policies and procedures are in place regarding contingency plans and their testing and revision that includes the following:</p> <ul style="list-style-type: none"> • Methods used to test the plan (component, system, or comprehensive) • Workforce members' roles and responsibilities in coordination of the test • How frequently tests will be conducted • How frequently contingency plans will be revised • Notification procedures 	Control implemented.
1.93	The BCP/DRP is tested on at least an annual basis.	Control implemented.
1.94	A documented BCP/DRP revision policy is in place to guide employees in revising the contingency plans.	Control implemented.
1.95	Management approves, reviews, and updates the BCP/DRP on an annual basis.	Control implemented.
§164.308(a)(7)(ii)(E): Assess the relative criticality of specific applications and data in support of other contingency plan components.		
1.96	Policies and procedures are in place to guide personnel in the assessment of the criticality of systems and applications that contain ePHI.	Control implemented.
1.97	The relative criticality of applications and data is formally documented.	Control implemented.
§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.		
1.98	A formal risk assessment is performed on at least an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Control implemented.
1.99	Internal vulnerability scans are performed on a monthly basis to identify potential infrastructure security vulnerabilities.	Control implemented.
1.100	An independent penetration test specialist performs a network penetration assessment of the production infrastructure on an annual basis to identify potential security vulnerabilities.	Control implemented.
1.101	<p>A central antivirus server is utilized to protect registered production Windows servers and workstations with the following configurations:</p> <ul style="list-style-type: none"> • Scan for updates to antivirus definitions and update registered clients on a real-time basis • Scan registered clients on a daily basis 	Control implemented.
1.102	<p>Documented policies and procedures are in place regarding technical and non-technical evaluations that includes the following:</p> <ul style="list-style-type: none"> • Workforce members' roles and responsibilities in the technical and nontechnical evaluation • Management involvement in the process and approval of technical and nontechnical evaluation • Coordination of technical and nontechnical evaluation among departments • Specification of how technical and nontechnical evaluation will be conducted • How technical and nontechnical evaluation findings will be addressed 	Control implemented.

#	Control Activity Specified by the Service Organization	Results
<p>§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. §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.</p>		
<p>Not applicable. LightEdge does not disclose ePHI data to business associates.</p>		
<p>§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).</p>		
<p>Not applicable. LightEdge does not disclose ePHI data to business associates.</p>		
<p>§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.</p>		
1.103	<p>Physical access policies and procedures are in place for areas that contain ePHI that includes the following:</p> <ul style="list-style-type: none"> • Workforce members' roles and responsibilities in facility access control procedures • Management involvement in the facility's access controls procedures • The process of how authorization credentials for facility access are issued • The process of removing workforce members' authorization credentials for physical access when such access it is no longer required • Identification of how visitors' access is monitored • Methods for controlling and managing physical access devices • Facilities and areas that have physical access control implemented to safeguard ePHI 	Control implemented.
1.104	Physical access rights to the areas that contain ePHI are reviewed on an annual basis to help ensure that physical access to data is restricted.	Control implemented.
1.105	Physical access requests are documented on a standard access request form and require the approval of management prior to access being granted.	Control implemented.
1.106	Requests to remove physical access privileges assigned to terminated employees are documented on a standardized access removal form.	Control implemented.
1.107	IT personnel revoke terminated employee physical access rights upon notification of employee termination.	Control implemented.
1.108	Security guards are in place to monitor the facility and data center during non-business hours.	Control implemented.
1.109	An alarm system is in place to monitor the facility and data center during non-business hours.	Control implemented.
1.110	Visitors to the corporate office facility are required to check in at the lobby before being escorted into the back-office area. Access to the back-office area is restricted via a badge access system.	Control implemented.
1.111	Visitors and vendors are required to present valid government-issued photo identification prior to being granted data center access.	Control implemented.
1.112	Visitors are required to sign a visitor log upon entering the main entrance of the data centers.	Control implemented.
1.113	Visitors are required to be escorted by an authorized employee while in the facility and data center.	Control implemented.
1.114	A badge access system is in place to control access into and throughout the facility and data center.	Control implemented.

#	Control Activity Specified by the Service Organization	Results
1.115	Management personnel assign access rights to employees for physical security zones through the use of predefined access groups.	Control implemented.
1.116	The data center utilizes a two-factor authentication system at the main entrance that requires an access code and badge access card credential for authorized entry into the data center.	Control implemented.
1.117	Access to physical areas that contain electronic information systems is restricted to badge access cards assigned to authorized personnel.	Control implemented.
Not applicable (Phoenix 1 Data Center). Digital Realty is responsible for restricting physical access to data center facilities that host the electronic information systems.		
§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.		
1.118	<p>A physical security contingency plan is in place to guide personnel in procedures to protect against disruptions caused by an unexpected event with elements that include the following:</p> <ul style="list-style-type: none"> • Identification of who will need access to ePHI in the event of a disaster • Backup up plan for access to the facility and/or ePHI • Workforce member roles and responsibilities from implementing the contingency plan for accessing ePHI in each department, unit, etc. • Procedures for accessing restored data at the alternate processing, storage, and work site • Procedures for the testing contingency operations 	Control implemented.
1.119	A contingency BCP/DRP is tested by personnel on at least an annual basis.	Control implemented.
Not applicable (Phoenix 1 Data Center). Digital Realty is responsible for restricting physical access to data center facilities that host the electronic information systems.		
§164.310(a)(2)(ii): Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.		
1.120	<p>A physical security plan is in place to guide personnel in procedures to protect against unauthorized physical access, tampering, or theft of ePHI with elements that include the following:</p> <ul style="list-style-type: none"> • Identification of the physical security measures in place to provide physical security protection for facilities and equipment • Workforce members' roles and responsibilities regarding the facility security plan • Inventory of the entity's facilities that house equipment that create, maintain, receive, and transmit ePHI 	Control implemented.
1.121	<p>Physical access policies and procedures are in place for areas that contain ePHI that includes the following:</p> <ul style="list-style-type: none"> • Workforce members' roles and responsibilities in facility access control procedures • Management involvement in the facility's access controls procedures • The process of how authorization credentials for facility access are issued • The process of removing workforce members' authorization credentials for physical access when such access it is no longer required • Identification of how visitors' access is monitored • Methods for controlling and managing physical access devices • Facilities and areas that have physical access control implemented to safeguard ePHI 	Control implemented.
1.122	Physical access requests are documented on a standard access request form and require the approval of management prior to access being granted.	Control implemented.

#	Control Activity Specified by the Service Organization	Results
1.123	Requests to remove physical access privileges assigned to terminated employees are documented on a standardized access removal form.	Control implemented.
1.124	IT personnel revoke terminated employee physical access rights upon notification of employee termination.	Control implemented.
1.125	Security guards are in place to monitor the facility and data center during non-business hours.	Control implemented.
1.126	An alarm system is in place to monitor the facility and data center during non-business hours.	Control implemented.
1.127	Visitors to the corporate office facility are required to check in at the lobby before being escorted into the back-office area. Access to the back-office area is restricted via a badge access system.	Control implemented.
1.128	Visitors and vendors are required to present valid government-issued photo identification prior to being granted data center access.	Control implemented.
1.129	Visitors are required to sign a visitor log upon entering the main entrance of the data centers.	Control implemented.
1.130	Visitors are required to be escorted by an authorized employee while in the facility and data center.	Control implemented.
1.131	A badge access system is in place to control access into and throughout the facility and data center.	Control implemented.
1.132	Management personnel assign access rights to employees for physical security zones through the use of predefined access groups.	Control implemented.
1.133	The data center utilizes a two-factor authentication system at the main entrance that requires an access code and badge access card credential for authorized entry into the data center.	Control implemented.
1.134	Access to physical areas that contain electronic information systems is restricted to badge access cards assigned to authorized personnel.	Control implemented.
1.135	Physical access rights to the areas that contain ePHI are reviewed on an annual basis to help ensure that physical access to data is restricted.	Control implemented.
Not applicable (Phoenix 1 Data Center). Digital Realty is responsible for restricting physical access to data center facilities that host the electronic information systems.		
§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.		
1.136	Physical access policies and procedures are in place for areas that contain ePHI that includes the following: <ul style="list-style-type: none"> • Workforce members' roles and responsibilities in facility access control procedures • Management involvement in the facility's access controls procedures • The process of how authorization credentials for facility access are issued • The process of removing workforce members' authorization credentials for physical access when such access it is no longer required • Identification of how visitors' access is monitored • Methods for controlling and managing physical access devices • Facilities and areas that have physical access control implemented to safeguard ePHI 	Control implemented.
1.137	Physical access requests are documented on a standard access request form and require the approval of management prior to access being granted.	Control implemented.
1.138	Requests to remove physical access privileges assigned to terminated employees are documented on a standardized access removal form.	Control implemented.

#	Control Activity Specified by the Service Organization	Results
1.139	IT personnel revoke terminated employee physical access rights upon notification of employee termination.	Control implemented.
1.140	Security guards are in place to monitor the facility and data center during non-business hours.	Control implemented.
1.141	An alarm system is in place to monitor the facility and data center during non-business hours.	Control implemented.
1.142	Visitors to the corporate office facility are required to check in at the lobby before being escorted into the back-office area. Access to the back-office area is restricted via a badge access system.	Control implemented.
1.143	Visitors and vendors are required to present valid government-issued photo identification prior to being granted data center access.	Control implemented.
1.144	Visitors are required to sign a visitor log upon entering the main entrance of the data centers.	Control implemented.
1.145	Visitors are required to be escorted by an authorized employee while in the facility and data center.	Control implemented.
1.146	A badge access system is in place to control access into and throughout the facility and data center.	Control implemented.
1.147	Management personnel assign access rights to employees for physical security zones through the use of predefined access groups.	Control implemented.
1.148	The data center utilizes a two-factor authentication system at the main entrance that requires an access code and badge access card credential for authorized entry into the data center.	Control implemented.
1.149	Access to physical areas that contain electronic information systems is restricted to badge access cards assigned to authorized personnel.	Control implemented.
1.150	Physical access rights to the areas that contain ePHI are reviewed on an annual basis to help ensure that physical access to data is restricted.	Control implemented.
Not applicable (Phoenix 1 Data Center). Digital Realty is responsible for restricting physical access to data center facilities that host the electronic information systems.		
§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).		
1.151	Documented physical security maintenance policies and procedures are in place to help ensure that physical components of the facility are repaired and maintained consistently.	Control implemented.
1.152	A ticketing system is utilized to document and track repairs and modifications to physical security components within the facility.	Control implemented.
Not applicable (Phoenix 1 Data Center). Digital Realty is responsible for restricting physical access to data center facilities that host the electronic information systems.		
§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.		
1.153	A documented workstation security policy is in place to describe the proper use of workstations and the handling of information maintained in the surroundings of workstations within the facilities.	Control implemented.
1.154	An inventory of workstations that may contain ePHI is maintained and updated by management.	Control implemented.
§164.310(c): Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.		
1.155	A documented workstation security policy is in place to describe the proper use of workstations and the handling of information maintained in the surroundings of workstations within the facilities.	Control implemented.

#	Control Activity Specified by the Service Organization	Results
1.156	Workstations are configured to lock and password protect the workstation after 10 minutes of inactivity.	Control implemented.
1.157	Disk encryption software is utilized on all workstations to help ensure that data is secured in the event that a workstation is lost or stolen.	Control implemented.
§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.		
1.158	A documented media policy is in place to guide personnel in the proper receipt and removal of hardware and electronic media that contain ePHI, into and out of a facility, and the movement of these items within the facility.	Control implemented.
Customer Responsibility. Customers are responsible for notifying LightEdge of requests to receive or remove hardware and electronic media that contain ePHI.		
§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.		
1.159	A documented technology equipment disposal policy is in place to guide personnel in the proper disposal of technology equipment with elements that include the following: <ul style="list-style-type: none"> How the disposal of ePHI and or the hardware or electronic media that stores ePHI is managed and documented Identification of how the sanitization process of information system media is managed and documented Workforce members' roles and responsibilities in the device and media disposal process Identification of how the disposition of previous stored ePHI and/or the hardware or electronic media is verified Identification of the types of devices and media that store ePHI 	Control implemented.
Customer Responsibility. Customers are responsible for notifying LightEdge of requests to receive or remove hardware and electronic media that contain ePHI.		
§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.		
1.160	A documented media reuse policy is in place to guide personnel in the proper removal of ePHI from electronic media before the media are made available for reuse.	Control implemented.
Customer Responsibility. Customers are responsible for notifying LightEdge of requests to remove ePHI from electronic media before the media are made available for reuse.		
§164.310(d)(2)(iii): Maintain a record of the movements of hardware and electronic media and any person responsible therefore.		
1.161	A centralized asset listing is used by management to track hardware and electronic media along with the person responsible for each piece of equipment.	Control implemented.
1.162	A documented hardware and electronic media movement policy is in place to guide personnel in the proper movement and accountability for media devices.	Control implemented.
§164.310(d)(2)(iv): Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.		
1.163	Documented backup policies and procedures are in place to create a retrievable exact copy of systems or data before movement of equipment.	Control implemented.
1.164	An automated backup system is in place to perform scheduled backups of systems or data before the movement of equipment as a component of the backup process.	Control implemented.

#	Control Activity Specified by the Service Organization	Results
1.165	An automated backup system is in place to perform scheduled backups of production servers on a daily basis.	Control implemented.
1.166	An automated backup system is configured to perform backups of production data to disk on a daily basis.	Control implemented.
1.167	The backup system is configured to automatically replicate backup data to a geographically separate location on a daily basis.	Control implemented.
§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).		
1.168	Documented policies and procedures are in place to guide personnel in the authorization of user accounts and account policy requirements.	Control implemented.
1.169	Documented policies and procedures are in place to guide personnel regarding access provisioning, modification, removal, and review.	Control implemented.
1.170	Access requests are documented on a standard access request form.	Control implemented.
1.171	Access modification requests are documented on a standard access request form.	Control implemented.
1.172	System owners revoke terminated employees' access to the in-scope systems as a component of the termination process.	Control implemented.
1.173	The in-scope systems are configured to authenticate users with a unique user account and enforce predefined user account and minimum password requirements.	Control implemented.
1.174	Access to systems that host ePHI is restricted to appropriate personnel.	Control implemented.
1.175	Managers review user access to the in-scope systems containing ePHI on at least an annual basis to help ensure that access correlates with employee job functions and duties.	Control implemented.
§164.312(a)(2)(i): Assign a unique name and/or number for identifying and tracking user identity.		
1.176	Documented policies and procedures are in place to guide personnel in the authorization of user accounts and account policy requirements.	Control implemented.
1.177	The in-scope systems are configured to authenticate users with a unique user account and enforce predefined user account and minimum password requirements.	Control implemented.
1.178	Access requests are documented on a standard access request form.	Control implemented.
§164.312(a)(2)(ii): Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.		
1.179	Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Control implemented.
§164.312(a)(2)(iii): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.		
1.180	Workstations are configured to lock and password protect the workstation after 10 minutes of inactivity.	Control implemented.
§164.312(a)(2)(iv): Implement a mechanism to encrypt and decrypt electronic protected health information.		
1.181	Encryption policies and procedures are in place to help ensure that the encryption and decryption of ePHI includes the use and management of the confidential process and key management.	Control implemented.
1.182	Encrypted VPN connections are used to help ensure that data being transmitted over public networks is secure.	Control implemented.
1.183	Web servers utilize TLS encryption for web communication sessions.	Control implemented.

#	Control Activity Specified by the Service Organization	Results
Customer Responsibility. Customers are responsible for ensuring ePHI data is encrypted at rest.		
§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.		
1.184	The in-scope systems are configured to log access related events including the following: <ul style="list-style-type: none"> · Account management · Logon events · Object access · Policy change · Privileged use 	Control implemented.
1.185	The in-scope systems are configured to automatically notify operations personnel in the event that an event triggers a predefined alert.	Control implemented.
§164.312(c)(1): Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.		
1.186	A policy is in place that documents the authentication and password requirements.	Control implemented.
1.187	The in-scope systems are configured to authenticate users with a unique user account and enforce predefined user account and minimum password requirements.	Control implemented.
1.188	The in-scope systems are configured to log access related events including the following: <ul style="list-style-type: none"> · Account management · Logon events · Object access · Policy change · Privileged use 	Control implemented.
1.189	The in-scope systems are configured to automatically notify operations personnel in the event that an event triggers a predefined alert.	Control implemented.
Customer Responsibility. Customers are responsible for ensuring ePHI data is encrypted at rest.		
§164.312(c)(2): Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.		
1.190	The in-scope systems are configured to log access related events including the following: <ul style="list-style-type: none"> · Account management · Logon events · Object access · Policy change · Privileged use 	Control implemented.
1.191	The in-scope systems are configured to automatically notify operations personnel in the event that an event triggers a predefined alert.	Control implemented.
1.192	Access to systems that host ePHI is restricted to appropriate personnel.	Control implemented.
§164.312(d): Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.		
1.193	A policy is in place that documents the authentication and password requirements.	Control implemented.
1.194	The in-scope systems are configured to authenticate users with a unique user account and enforce predefined user account and minimum password requirements.	Control implemented.

#	Control Activity Specified by the Service Organization	Results
§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.		
1.195	<p>Encryption policies and procedures are in place to help ensure that technical security controls are implemented to guard against unauthorized access to ePHI transmitted over electronic communications networks with elements that include the following:</p> <ul style="list-style-type: none"> • Identification of the various methods, devices, and networks used to electronically transmit ePHI • The procedures to evaluate and select appropriate technical controls to secure ePHI transmitted across all of its devices and networks • Identification of the technical security controls implemented to guard against unauthorized access to ePHI transmitted over electronic communication networks 	Control implemented.
1.196	Encrypted VPN connections are used to help ensure that data being transmitted over public networks is secure.	Control implemented.
1.197	Web servers utilize TLS encryption for web communication sessions.	Control implemented.
§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.		
1.198	<p>The in-scope systems are configured to log access related events including the following:</p> <ul style="list-style-type: none"> • Account management • Logon events • Object access • Policy change • Privileged use 	Control implemented.
1.199	The in-scope systems are configured to automatically notify operations personnel in the event that an event triggers a predefined alert.	Control implemented.
1.200	Encrypted VPN connections are used to help ensure that data being transmitted over public networks is secure.	Control implemented.
1.201	Web servers utilize TLS encryption for web communication sessions.	Control implemented.
Customer Responsibility. Customers are responsible for ensuring ePHI data at rest is encrypted and for documenting electronic transmission policies and procedures to help ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of and means of detecting if transmitted ePHI has been improperly modified.		
§164.312(e)(2)(ii): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.		
1.202	<p>Encryption policies and procedures are in place with elements that include the following:</p> <ul style="list-style-type: none"> • Type(s) and documentation of encryption technology used to secure electronically transmitted ePHI • How the confidential processes or keys used for encryption are managed and protected • How access to modify or create keys is restricted to appropriate personnel • Identify when it is appropriate to encrypt ePHI 	Control implemented.
1.203	Encrypted VPN connections are used to help ensure that data being transmitted over public networks is secure.	Control implemented.
1.204	Web servers utilize TLS encryption for web communication sessions.	Control implemented.

#	Control Activity Specified by the Service Organization	Results
	Customer Responsibility. Customers are responsible for ensuring ePHI data is encrypted at rest.	
	§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.	
	Not applicable. LightEdge does not disclose ePHI data to business associates.	
	§164.314(a)(2)(i)(A): The contract must provide that the business associate will— (A) Comply with the applicable requirements of this subpart;	
	Not applicable. LightEdge does not disclose ePHI data to business associates.	
	§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.	
	Not applicable. LightEdge does not disclose ePHI data to business associates.	
	§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	
	Not applicable. LightEdge does not disclose ePHI data to business associates.	
	§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).	
	Not applicable. LightEdge is not a covered entity.	
	§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.	
	Not applicable. LightEdge does not disclose ePHI data to business associates.	
	§164.314(a)(b)(1): Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii), or as authorized under §164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	
	Not applicable. LightEdge is not a health plan.	
	§164.314(b)(2)(i): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan.	
	Not applicable. LightEdge is not a health plan.	
	§164.314(b)(2)(ii): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (ii) Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures.	
	Not applicable. LightEdge is not a health plan.	
	§164.314(b)(2)(iii): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information.	
	Not applicable. LightEdge is not a health plan.	
	§164.314(b)(2)(iv): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (iv) Report to the group health plan any security incident of which it becomes aware.	
	Not applicable. LightEdge is not a health plan.	
	§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.	

#	Control Activity Specified by the Service Organization	Results
1.205	Policies and procedures are in place to address specific policies and procedures needed to comply with the standards, implementation specification or other requirements of the HIPAA Security Rule.	Control implemented.
§164.316(b)(1): (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record or the action, activity, or assessment.		
1.206	Policies and procedures are in place that address LightEdge maintaining written policies and procedures related to the security rule and written documents of (if any) actions, activities, or assessments required of the HIPAA Security Rule.	Control implemented.
§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.		
1.207	Policies and procedures are in place that address required documentation being retained for six years from the date of its creation or the date when it last was in effect.	Control implemented.
1.208	Action, activity, or assessment documentation is maintained for six years from the date of its creation or the date when it last was in effect.	Control implemented.
§164.316(b)(2)(ii): Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.		
1.209	Policies and procedures are made available to the workforce members responsible for implementing the pertaining procedures via the company intranet.	Control implemented.
§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.		
1.210	Policies and procedures are in place that dictate the review and update of HIPAA Security Rule related policies and procedures on at least an annual basis.	Control implemented.
1.211	The director of business operations and the chief security officer review and update Security Rule policies and procedures on an annual basis, and as needed, in response to environmental or operational changes affecting the security of ePHI.	Control implemented.

HITECH BREACH NOTIFICATION RULE

#	Control Activity Specified by the Service Organization	Results
§164.414(a): Administrative Requirements. A covered entity is required to comply with the administrative requirements of §164.530(b), (d), (e), (g), (h), (i), and (j) with respect to 45 CFR Part 164, Subpart D ("the Breach Notification Rule"). [Training, complaints to the covered entity, sanctions, refraining from intimidating or retaliatory acts, waiver of rights, policies and procedures, and documentation]		
Not applicable. LightEdge is not a covered entity.		
§164.530(b): Training. All workforce members must receive training pertaining to the Breach Notification Rule.		
2.01	Policies and procedures are in place that address training for workforce on the Breach Notification Rule.	Control implemented.
2.02	Employees complete training upon hire and on an annual basis thereafter to understand their obligations and responsibilities to comply with the HITECH Breach Notification Rule.	Control implemented.

#	Control Activity Specified by the Service Organization	Results
	§164.530(d): Complaints. All covered entities must provide a process for individuals to complain about its compliance with the Breach Notification Rule.	
	Not applicable. LightEdge is not a covered entity.	
	§164.530(e): Sanctions. All covered entities must sanction workforce members for failing to comply with the Breach Notification Rule.	
	Not applicable. LightEdge is not a covered entity.	
	§164.530(g): Refraining from Retaliatory Acts. All covered entities must have policies and procedures in place to prohibit retaliatory acts.	
	Not applicable. LightEdge is not a covered entity.	
	§164.530(h): Waiver of Rights. All covered entities must have policies and procedures in place to prohibit it from requiring an individual to waive any rights under the Breach Notification Rule as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.	
	Not applicable. LightEdge is not a covered entity.	
	§164.530(i): Policies and Procedures. All covered entities must have policies and procedures that are consistent with the requirements of the Breach Notification Rule.	
	Not applicable. LightEdge is not a covered entity.	
	§164.530(j): Documentation. All covered entities must have policies and procedures in place for maintaining documentation.	
	Not applicable. LightEdge is not a covered entity.	
	§164.402: Definitions: Breach - Risk Assessment. Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of this part which compromises the security or privacy of the PHI. (2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors: (i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (ii) The unauthorized person who used the PHI or to whom the disclosure was made; (iii) Whether the PHI was actually acquired or viewed; and (iv) The extent to which the risk to the PHI has been mitigated.	
2.03	Policies and procedures are in place to guide personnel in conducting a risk assessment for incidents that result in impermissible acquisition, access, use, or disclosure of PHI that includes the following factors: <ul style="list-style-type: none"> • The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification • The unauthorized person who used the PHI or to whom the disclosure was made • Whether the PHI was actually acquired or viewed • The extent to which the risk to the PHI has been mitigated 	Control implemented.
2.04	A risk assessment is performed to determine whether a notification must be provided when an impermissible acquisition, access, use, or disclosure of PHI in accordance with policies and procedures.	Control implemented.

#	Control Activity Specified by the Service Organization	Results
	<p>§164.402: Definitions: Breach Exceptions - Unsecured PHI. Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of this part which compromises the security or privacy of the PHI. (1) Breach excludes: (i) Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.(ii) Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part. (iii) A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. (2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;(iii) Whether the protected health information was actually acquired or viewed; and(iv) The extent to which the risk to the protected health information has been mitigated. Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.</p>	
2.05	<p>Policies and procedures are in place to guide personnel in conducting a risk assessment for incidents that result in impermissible acquisition, access, use, or disclosure of PHI that includes the following factors:</p> <ul style="list-style-type: none"> • The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification • The unauthorized person who used the PHI or to whom the disclosure was made • Whether the PHI was actually acquired or viewed • The extent to which the risk to the PHI has been mitigated 	Control implemented.
2.06	<p>A risk assessment is performed to determine whether a notification must be provided when an impermissible acquisition, access, use, or disclosure of PHI in accordance with policies and procedures.</p>	Control implemented.
<p>§164.404(a)(1): Notice to Individuals. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach. (2) Breaches treated as discovered. For purposes of paragraph (a)(1) of this section, §164.406(a), and §164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).</p>		
<p>Not applicable. LightEdge is not a covered entity.</p>		
<p>§164.404(b): Timeliness of Notifications. Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.</p>		
<p>Not applicable. LightEdge is not a covered entity.</p>		
<p>§164.404(c)(1): Content of Notification. The notification required by paragraph (a) of this section shall include, to the extent possible:(A) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;(B) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);(C) Any steps the individual should take to protect themselves from potential harm resulting from the breach;(D) A brief description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches; and(E) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.(2) The notification required by paragraph (a) of this section shall be written in plain language.</p>		
<p>Not applicable. LightEdge is not a covered entity.</p>		

#	Control Activity Specified by the Service Organization	Results
	<p>§164.404(d): Methods of Notification. The notification required by paragraph (a) of this section shall be provided in the following form:(1) (i) Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information becomes available. (ii) If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under §164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual is required. The notification may be provided in one or more mailings as information is available. (2) Substitute notice. In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual under this paragraph (d)(1)(i) of this section, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).(i) In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then substitute notice may be provided by an alternative form of written notice, telephone, or other means.(ii) In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) Include a toll-free number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.(3) In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.</p>	
	<p>Not applicable. LightEdge is not a covered entity.</p>	
	<p>§164.406(a): Notification to the Media. For a breach of unsecured PHI involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in §164.404(a)(2), notify prominent media outlets serving the State or jurisdiction.(b)Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.(c) The content of the notification required by paragraph (a) of this section shall meet the requirements of §164.404(c).</p>	
	<p>Not applicable. LightEdge is not a covered entity.</p>	
	<p>§164.408: Notification to the Secretary. (a) A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in §164.404(a)(2), notify the Secretary.(b) For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in §164.412, provide the notification required by paragraph (a) of this section contemporaneously with the notice required by §164.404(a) and in the manner specified on the HHS Web site.(c) For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches discovered during the preceding calendar year, in the manner specified on the HHS Web site.</p>	
	<p>Not applicable. LightEdge is not a covered entity.</p>	
	<p>§164.410: Notification by a Business Associate. (a) Standard. (1) General Rule. A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach. (2) For purposes of paragraph (a)(1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).(b) Except as provided in §164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.(c)(1) The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach. (2) A business associate shall provide the covered entity with any other available information that the covered entity is required to include in notification to the individual under §164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.</p>	
2.07	<p>Management notifies a covered entity regarding any known or suspected breaches within 60 calendar days and includes the identification of each individual whose unsecured protected health information has been or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.</p>	Control implemented.

#	Control Activity Specified by the Service Organization	Results
<p>§164.412: Law Enforcement Delay. If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made verbally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.</p>		
2.08	Policies and procedures are in place to guide workforce personnel on how to they would respond to a law enforcement statement that a notice or posting would impede a criminal investigation or damage national security.	Control implemented.
2.09	Legal Counsel comply with law enforcement delay requests for breach notifications.	Control implemented.
<p>§164.414(b): Burden of proof. In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by the subpart or that the use or disclosure did not constitute a breach as defined at §164.402.</p>		
2.10	Documented policies and procedures are in place to help ensure that notifications are made as required or that an impermissible use or disclosure did not constitute a breach.	Control implemented.
2.11	A risk assessment is performed to determine whether a notification must be provided when an incident results in impermissible acquisition, access, use, or disclosure.	Control implemented.
2.12	A data breach notification policy and breach investigation incident report template are in place to guide personnel in the breach notification process.	Control implemented.