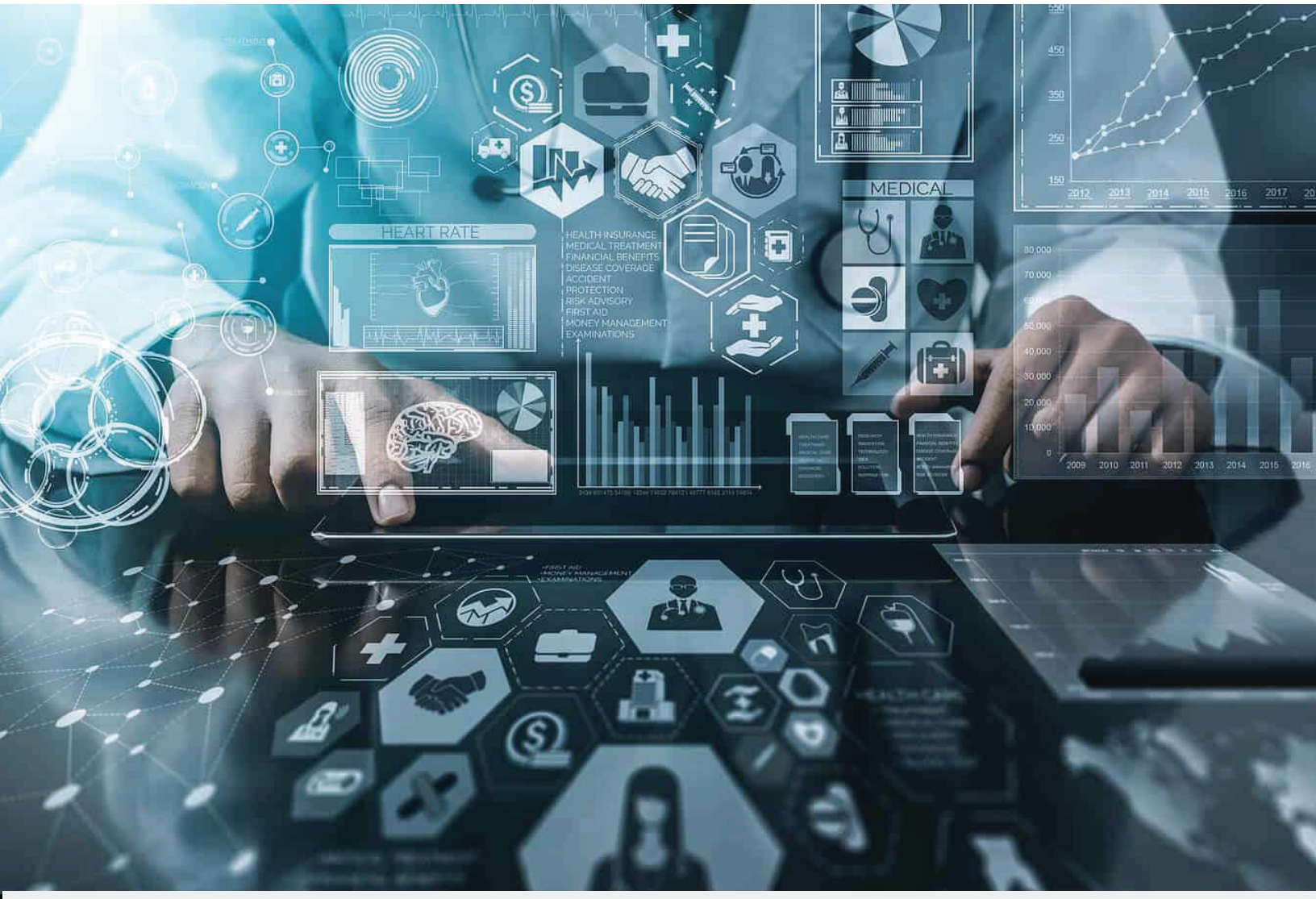
linford&co llp
cpa firm

Ledidi



HIPAA

REPORT ON COMPLIANCE WITH THE HIPAA SECURITY AND BREACH NOTIFICATION RULES

AS OF APRIL 30, 2025

Ledidi AS

Report on Ledidi's Description of Its Ledidi Core Services and on Management's Assertion Related to Compliance with HIPAA

Table of Contents

Table of Contents (continued)

linford&co llp
cpa firm

▪ linford&co llp
1550 wewatta st, 2nd floor
denver, co 80202

▪ tel: +1 (720) 330 7201
email: info@linfordco.com
www.linfordco.com

Section I – Independent Service Auditor's Report

To the Board of Directors of Ledidi AS:

Scope

We have examined Ledidi AS' (Ledidi or the Company) management assertion, included in Section II of the accompanying *Report on Ledidi's Description of Its Ledidi Core Services and on Management's Assertion Related to Compliance with HIPAA*, that Ledidi complied with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule and Breach Notification Rule requirements (collectively, "the specified requirements" or "the HIPAA requirements"), as of April 30, 2025. Ledidi's management is responsible for Ledidi's compliance with the specified requirements. Our responsibility is to express an opinion on management's assertion about Ledidi's compliance based on our examination.

Ledidi uses Amazon Web Services, Inc. (AWS), a subservice organization, to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Ledidi, to achieve Ledidi's service commitments and system requirements based on the applicable HIPAA requirements. The description presents Ledidi's controls, the applicable HIPAA requirements, and the types of complementary subservice organization controls assumed in the design of Ledidi's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Ledidi, to achieve Ledidi's service commitments and system requirements based on the applicable HIPAA requirements. The description presents Ledidi's controls, the applicable HIPAA requirements, and the complementary user entity controls assumed in the design of Ledidi's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform the examination to obtain reasonable assurance about whether Ledidi's assertion about compliance with the specified requirements is fairly stated, in all material respects. Accordingly, our examination involved procedures to obtain and examine, on a test basis, evidence about Ledidi's compliance with the specified requirements and performing such other procedures we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion. Our examination does not provide a legal determination on Ledidi's compliance with the HIPAA requirements.

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

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon. The specific controls tested for the suitability of design and the nature, timing, and results of those procedures are presented in Section IV of this report titled, *Independent Service Auditor's Description of Tests of Controls and Results*.

Opinion

In our opinion, management's assertion that Ledidi complied with the HIPAA requirements, as of April 30, 2025, was fairly stated, in all material respects, based on the description of controls set forth in Sections III and IV of this report, our tests of controls and results set forth in Section IV of this report, and the HIPAA requirements set forth in Section V of this report.

linford&co llp

May 2, 2025
Denver, Colorado

Section II – Assertion of Ledidi Management

May 2, 2025

Ledidi AS (Ledidi or the Company) is responsible for establishing and maintaining effective controls over its Ledidi core services. The controls are designed to provide reasonable assurance to executive management and the board of directors that the HIPAA control requirements contained in Section V of this report are achieved based on the identified controls in Section IV of this report.

Ledidi uses Amazon Web Services, Inc. (AWS), a subservice organization, to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Ledidi, to achieve Ledidi's service commitments and system requirements based on the applicable HIPAA requirements. The description presents Ledidi's controls, the applicable HIPAA requirements, and the types of complementary subservice organization controls assumed in the design of Ledidi's controls. The description does not disclose the actual controls at the subservice organization.

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

Because of inherent limitations in any control—no matter how well designed—error or fraud may occur and not be detected, including the possibility of the circumvention or overriding of controls. Even effective controls can provide only reasonable assurance with respect to the achievement of any requirement. Further, because of changes in conditions, the effectiveness of controls may vary over time.

Management has identified the HIPAA requirements in Section V of this report and related controls included in Section IV of this report as the basis for its assertion. Management's description of its Ledidi core services and entity level controls is contained in Section III of this report.

Management believes that as of April 30, 2025, its controls over its Ledidi core services were effective in providing reasonable assurance that the HIPAA requirements contained in Section V were achieved and, accordingly, that the Company is materially compliant with the HIPAA Security Rule and Breach Notification Rule requirements.

Danckert Mellbye
Chief Operating Officer

Section III – Ledidi's Description of Its Ledidi Core Services

Overview of Operations

Overview of the Organization

Ledidi is a software company providing a platform that allows users to capture and collect data, perform statistical and graphical data analysis, and collaborate with other users. The users of the platform are primarily medical and life science professionals that use the platform for medical and scientific research purposes.

System Description

Ledidi core services are delivered by the Ledidi Core platform that provides a secure research environment offering an end-to-end solution from the point of loading research data, which may be subject to HIPAA requirements, through analysis and final project output. Ledidi core services provide the tools to take raw data and manipulate and analyze it into the needed format and outcome for the project at hand. Ledidi provides for the capabilities of study design, data capture, statistical analysis, and data visualization.

Components of the System Used to Provide the Services

The system used by Ledidi to deliver the Ledidi core services is comprised of a combination of components that include the products and the data processed, but also extends to the underlying infrastructure, subservice organization's services supporting the platform, the Company's employees and contractors, as well as the policies and procedures followed to maintain the security of the Ledidi core services and client data. The following is a summary of the components that comprise the system. Specific processes and controls relevant to the HIPAA requirements are described in the remainder of this section of the report.

Infrastructure

Ledidi's system is a Software-as-a-Service (SaaS) cloud-based system. The primary components of the system are built on top of AWS.

Subservice Organization: AWS is the principal subservice organization used by Ledidi. Ledidi uses the subservice organization to support, build, manage, monitor, and maintain its infrastructure. AWS hosts Ledidi's production IT environment and provides certain managed services including secondary data backup services and virtual private network. AWS undergoes an annual Type II SOC 2 examination and the report may be obtained directly from them. Ledidi obtains and reviews the SOC 2 report provided by AWS related to their hosting operations to determine whether controls are designed and operating effectively. Additionally, any listed complementary user entity controls in the AWS SOC report are also reviewed and addressed by Ledidi.

Ledidi utilizes Amazon RDS and PostgreSQL for the production database and storage of client data. The database and data that resides in it is encrypted at rest. Complex passwords and multifactor authentication are required for Ledidi personnel to access the Ledidi environment.

Software

The Ledidi core services are developed and maintained by Ledidi personnel. The software engineering team enhances and maintains the Ledidi core services to provide the current services and future enhancements to its user entities. Access to the Ledidi core services is governed by the principle of least privilege. User entities are, in general, responsible for identifying the access needs for their users and for the security of those devices used to access the Ledidi core services. Complementary user entity controls are noted within this description (Section III) to highlight control activities that Ledidi believes should be considered and/or present at each user entity of its Ledidi core services.

People

Ledidi has a staff of personnel organized into functional areas that enable the execution of authorities, responsibilities, and the flow of information in the support of the achievement of business goals and objectives.

Data

Sensitive client data is stored within the Ledidi Core platform's production databases. Ledidi has implemented security measures to protect the confidentiality of sensitive client data. Access to data subject to HIPAA is restricted to authorized personnel who have a need to access such data. Ledidi has implemented logical data partitioning measures to prevent unauthorized access to data across clients using Ledidi's hosted SaaS platform. Security measures include encrypting data at rest and securing data transmissions by utilizing Transport Layer Security (TLS) and industry standard encryption.

Policies and Procedures

Ledidi has established policies and procedures that govern the development, usage, maintenance, support, and security of the Ledidi core services. Ledidi makes these internal policies and procedures, including security policies, available to its personnel via an internal company site to provide direction regarding their responsibilities related to the function of internal control.

Principal Service Commitments and System Requirements

Ledidi designs its processes and procedures to meet objectives for its Ledidi core services. Those objectives are based on the service commitments that Ledidi makes to user entities, the laws and regulations that govern the provision of Ledidi services, and the financial, operational, and compliance requirements that Ledidi has established for its services.

Security commitments to user entities are documented and communicated in their client agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- ✓ Security principles within the fundamental design of the Ledidi core services are implemented to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- ✓ Controlled access to the Ledidi core services and the supporting infrastructure.
- ✓ Segregation of client data.
- ✓ Use of encryption technologies to protect client data both at rest and in transit.

Ledidi establishes operational requirements that support the achievement of security commitments and other system requirements. Such requirements are communicated in Ledidi's system policies and procedures, system design documentation, and contracts with clients. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal networks are managed, and how employees are hired and trained.

Relevant Aspects of the Control Environment, Risk Assessment, Information and Communication, Monitoring, and Control Activities Relevant to the HIPAA Requirements

Note: Parenthetical references have been included in the following narratives as a cross reference to the applicable control activities included in Section IV of this report.

A company's entity-level controls reflect the overall attitude, awareness, and actions of management and others concerning the importance of controls and the emphasis given to controls in the company's policies, procedures, methods, and organizational structure. Entity-level controls are not specific to any individual transaction but apply to the company as a whole. These types of controls are necessary to facilitate the proper functioning of activity-level controls supporting Ledidi's core services. Throughout this section, there will be a description of the five components of internal control (control environment, risk assessment, information and communication, monitoring, and control activities) as they relate to the services Ledidi provides to its clients.

The controls supporting the specified requirements were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. HIPAA requirements and controls designed, implemented, and operated to meet them monitor that the system is protected against unauthorized access (both physical and logical). Entity-level controls and specific control activities supporting the applicable HIPAA requirements are provided in the descriptions of this section of the report, and in *Section IV – Independent Service Auditor's Description of Tests of Controls and Results.*

Control Environment

A board of directors, consisting of internal and external individuals, exercises oversight of Ledidi's strategic direction, operational performance, and internal control **(1.1)**. In addition, Ledidi has an executive management team that guides the Company and sets the tone at the top of the organization that is followed

by all employees. The tone is demonstrated through their directives, actions, and behavior, and highlights the importance of integrity and ethical values to support the functioning of the system of internal control. The executive management team meets on a weekly basis **(1.2)**.

To help employees understand expectations, executive management has established Ledidi's Quality Assurance and Internal Control System (LICS). Ledidi's LICS applies to all full-time, part-time, and contractor staff and includes the following sections: goals and annual plan, security, code of conduct, disciplinary process, and reporting violations **(1.3)**.

Continuous Independent Compliance and Security Monitoring: Ledidi has established an internal compliance function and supporting tools which monitor the Ledidi control environment and alerts management when internal control and security issues arise **(1.4)**.

Organizational Structure: Management has established structures, reporting lines, and appropriate authorities in the pursuit of Ledidi's business objectives. The structures, reporting lines, and authority are communicated through management's operational style, the organizational structure, policies and procedures, and employee job descriptions. Ledidi's organizational structure defines authorities across the Company to facilitate information flow and establish responsibilities **(1.5)**. To increase the operational effectiveness of employees within this structure, every position has a job description so that individuals understand their responsibilities **(1.6)**. The role of HIPAA Security Officer has been assigned and communicated throughout the organization. The HIPAA Security Officer is responsible for the security of Ledidi's systems including security relating to HIPAA compliance **(1.7)**.

Hiring: When a position is open at Ledidi, a job description and listing will be posted on Ledidi's website, as well as on other job forums. Additionally, Ledidi sources candidates via referrals. Resumes of applicants are received and reviewed by the hiring manager. The interview process is tailored to match the position being hired for and is a several stage process. Applicants for full-time employment at Ledidi are required to complete a successful reference check as part of the terms of their employment **(1.8)**. As part of the hiring process, applicants are required to sign an employee contract that contains a confidentiality agreement **(1.9)**. An onboarding checklist is completed to monitor completion of employment documentation and acknowledgment of Ledidi's LICS and assigned policies **(1.10)**.

New Hire Training: New hires are required to complete Ledidi security awareness training and HIPAA training and sign the Health, Environment, & Security (HES) Declaration at the start of their position **(1.11)**.

Performance and Feedback: Ledidi evaluates competence across the entity in relation to established policies and practices and acts, as necessary, to address shortcomings. Employee performance and feedback reviews are performed at least annually **(1.12)**. Ledidi believes feedback is forward-looking and is information that someone can use to grow and develop. Performance assessments, however, look to the past to discover how an individual performed over the last six months. Feedback is provided on an ongoing basis and formally on a biannual basis. As part of the terms of the employment agreement with individuals, Ledidi maintains the right to discipline or terminate individuals based on a pattern of poor job performance.

Information and Communication

Internal Control Monitoring: Ledidi uses a variety of methods to monitor production systems and internal controls to support the functioning of internal controls. The methods include a compliance function for monitoring internal controls relevant to security compliance, as well as application and infrastructure monitoring tools and penetration testing.

Internal Communication: Ledidi maintains policies to communicate HIPAA security and privacy responsibilities to Ledidi personnel **(2.1)**. The policies include objectives and responsibilities for internal control necessary to support the functioning of internal control. Policies are reviewed at least annually and updated, as necessary. Ledidi uses an internal communication tool to distribute policies and periodic security reminders to employees including responsibilities related to security **(2.2)**. In addition, the policies are available for all employees to reference as needed.

Annual Security Awareness Training: To assist with Ledidi's commitments to security and HIPAA compliance, Ledidi management provides annual security awareness training and HIPAA training for all employees that covers information security, data protection, and confidentiality of client information **(2.3)**.

Service Offering and Service Agreement: Ledidi has created a high-level overview of the Ledidi system used to describe the services provided to the clients that Ledidi serves **(2.4)**. Ledidi and its clients' responsibilities and commitments regarding the acceptable use of the Ledidi system and Protected Health Information (PHI), as applicable, are included within the Ledidi Enterprise Agreement and Terms of Service, which clients must agree to before using the Ledidi software **(2.5)**. For any service provider handling PHI on behalf of Ledidi, a BAA (Business Associate Addendum) is also required to be executed **(2.6)**.

Complementary User Entity Controls: *User entities are responsible for executing any required contractual obligations per their regional regulations and/or requirements.*

Incident Reporting: Ledidi has provided methods to clients and employees to report failures, incidents, concerns, or other complaints related to the services or systems provided by Ledidi in the event there are problems **(2.7)**. Ledidi personnel may contact their supervisor or the Compliance Officer to report important matters requiring attention. Ledidi has established an incident procedure to define the process for handling incidents and roles and responsibilities for the personnel responding to the incidents.

Risk Assessment

Ledidi Risk Assessment and Management Program: Ledidi's risk assessment procedure describes the processes Ledidi has in place to identify new business and technical risks and how to achieve the desired level of risk **(3.1)**. The procedure document designates responsibility for risk management at Ledidi and outlines the process for identifying and addressing risks to the confidentiality, integrity, and security of client data that Ledidi accesses, stores, and transmits. The policy is made available to all employees through the Company's policy repository **(3.2)**. Key business and operational risks are closely monitored,

particularly those related to the security of Ledidi's production environment, as these are especially critical risks that have the potential to affect the services provided to clients. Ledidi also mitigates business risks by adhering to industry practices to reduce risks related to the system.

Principles: Ledidi specifies risk management objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. Ledidi's primary duty is to maintain the security of critical systems and customer data. The duty to maintain a secure and available infrastructure requires Ledidi to identify and manage risks.

Risk Management Oversight: Overall, the execution, development, and implementation of risk assessments and remediation programs is the joint responsibility of Ledidi's Chief Operating Officer, Chief Technology Officer, Chief Product Officer, and the Compliance Officer. All departments and employees are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Annually, the risks identified are formally documented in a risk assessment matrix **(3.3)**. Each risk is assessed and given a risk rating. Risk owners work with the Compliance Officer in the development of a risk treatment plan per risk assessment performed and the risk assessment is reviewed by Ledidi management **(3.4)**.

Supplier Risk Management: Ledidi relies on suppliers to perform a variety of services, some of which are critical for operations. Ledidi aims to manage its relationship with suppliers and minimize the risk associated with engaging third parties to perform services. The supplier management procedures provide a framework for managing the life cycle of supplier relationships **(3.5)**. Risk assessments for suppliers are covered under Ledidi's supplier management program, which includes a risk assessment targeted at a particular suppliers' security and controls.

Fraud Risk: Ledidi has considered the potential for fraud when assessing risks to the achievement of objectives **(3.6)**.

Change Identification and Risk Assessment: Ledidi's risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates **(3.7)**.

Monitoring Activities

Application Logging and Monitoring: Ledidi uses AWS monitoring tools to monitor application health and the monitoring tool alerts system administrators when the application is not operating within defined boundaries **(4.1)**. Ledidi uses various third-party tools for monitoring. When alerts from the tools are received, they are followed up on until they are resolved.

Infrastructure Logging and Monitoring: Ledidi logs authentication, availability, and error events and uses tools for infrastructure monitoring **(4.2)**. Every authentication event to the application and infrastructure records a log event that may be used later for forensic purposes to research security incidents. Clients of Ledidi may also enter service tickets regarding potential issues they are experiencing. The client-submitted tickets are addressed by Ledidi personnel **(4.3)**.

Vulnerability Management: Ledidi has implemented steps within the change management process to test for security vulnerabilities that could impact operations of the Ledidi core services offering **(4.4)**. Should errors or vulnerabilities be identified during the testing, the change would be held until resolved.

Penetration Testing: Ledidi annually has a third-party application penetration test performed and issues identified during the test are remediated, as needed **(4.5)**.

Control Activities

Control activities are the specific functions performed by Ledidi management and employees to address the individual risks associated with the achievement of the Company's objectives. Properly functioning control activities support company operations and can be objectively viewed and independently tested. Control activities can take the form of automated and/or manual controls and function in a combination of systems and business processes.

Ledidi's appointed Compliance Officer, Data Protection Officer, and HIPAA Security Officer oversee the compliance program for the Company. Part of this oversight includes the establishment of policies and procedures to manage and direct company activity and to allow for periodic assessments of adherence to the policies and procedures **(5.1)**. In addition to developing policies and procedures, Ledidi's management also segregates responsibilities and duties across the organization to mitigate risks to the services provided to its clients and to the Ledidi Core platform **(5.2)**.

Ledidi has established a compliance program for management and monitoring of key practices and control points with key components of compliance, HIPAA, and security **(5.3)**. The compliance program includes monitoring of key activity and tracking of activity through a non-conformity register **(5.4)**. Meetings are held to review identified company activities, current status, and remediation activities **(5.5)**. Results of these compliance activities are presented at company management meetings **(5.6)**. Action is taken to address concerns as considered necessary as well as updates and additions made to the compliance program.

Information Security

Ledidi System Access and Authorization Control Policy: Ledidi employees and contractors have limited access to Ledidi systems and applications. Access is provisioned on a minimum-necessary (least-privilege) basis. Ledidi's system access procedures document the requirements for registering and authorizing employees and contractors prior to being issued system credentials and granted the ability to access the system **(6.1)**.

Employee Access to Ledidi Systems: Access to Ledidi systems and third-party accounts owned by Ledidi are only granted on a need-to-use basis, as defined by the responsibilities of the position held and the duties of the position. Access control and management is divided into multiple phases of the account life cycle, which include creation, privilege management, account audit, revocation – role changes and termination, authentication, guest access, disciplinary action, and responsibility.

Authorization – Role Based Access Control: Ledidi employees and contractors are granted access to Ledidi systems according to their role and/or team **(6.2)**. The executive team and team managers are jointly responsible for maintaining a list of roles and associated access scope for team members. The COO is the owner of the onboarding process and the Compliance Officer is responsible for adherence to the procedure.

User Provisioning and Deprovisioning: Ledidi has implemented role-based security to limit and control access within Ledidi's production environment. Access is provisioned by the security officer based on notification received from the CEO authorizing such access **(6.3)**. Access approval is based on the role and responsibilities of the user, and a policy of least privilege. The individual requesting access cannot approve their own access. In addition, Ledidi employees and contractors must accept the Company's acceptable use policy upon being hired **(6.4)**. When an employee or contractor is terminated, the Security team revokes production access upon termination **(6.5)**.

Complementary User Entity Controls: *User entities are responsible for provisioning and deprovisioning user access to authorized individuals according to the principle of least privilege.*

Account Audit: On a semi-annual basis, the system owners conduct a user appropriateness review of access to Ledidi resources to validate internal user access is commensurate with job responsibilities **(6.6)**. This review is performed as part of the overall company risk assessment activities.

Complementary User Entity Controls: *User entities are responsible for periodically reviewing user access and access permissions to determine whether access is limited to appropriate personnel.*

Complementary User Entity Controls: *User entities are responsible for configuring strong password complexity requirements when using their own authentication method into the Ledidi environment.*

Complementary User Entity Controls: *User entities are responsible for configuring multifactor authentication when using their own authentication method into the Ledidi environment.*

Administrator and Remote Access: Administrator-level access privileges to the production environment are restricted to only those individuals who require such access to perform their respective job functions **(6.7)**. Access is limited to certain individuals who require the ability to add, delete, and modify users' access to the production system.

Passwords: Ledidi has developed a password policy to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change. Password parameters to production systems enforce standards for minimum length and complexity **(6.8)**. Remote access to the production infrastructure is limited to authorized individuals and communications are encrypted **(6.9)**.

Access to Client Data: Client data is stored within Ledidi's production database instance. Access to client data within the Ledidi production database by Ledidi employees is restricted to authorized users **(6.10)**. In addition, client users have access to their data only and no other clients' data **(6.11)**.

Encryption of Client Data: Ledidi understands the sensitivity of its clients' data and has therefore implemented security controls to protect the confidentiality of the data. Client data within Ledidi's production databases is encrypted **(6.12)**.

Infrastructure Authentication: Multifactor authentication is required for access to the production environment **(6.13)**.

Workstation Use and Security: The Company's policies and procedures provide guidance to its personnel concerning the physical safeguarding of workstations with access to the IT environment and information relevant to HIPAA requirements for company devices **(6.14)**. The guidance applies to devices such as a Windows or MacBook laptop, tablet, or other electronic devices (e.g., fixed workstation, portable workstation/laptop computer, tablet computer, smartphone, etc.) and to locations such as office, home, public place, etc. The guidance also includes access to physical and logical information and data subject to HIPAA requirements. User workstations are required to be encrypted, maintain current patching and operating systems, have antimalware software installed, and configured to automatically lock after five minutes of inactivity **(6.15)**.

Physical Access to Facilities and Information: Ledidi is headquartered in Oslo, Norway, and has a physical office located in the Oslo Science Park. Oslo Science Park manages access to the facility and the Ledidi office via keycard access. Only authorized Ledidi personnel have a keycard to the Ledidi office **(6.16)**. A personal pin code, in addition to the keycard, is required to enter the facility after business hours. All infrastructure, including that which contains client data and/or electronic PHI (ePHI), is housed entirely within subservice provider AWS' environment. Physical and environmental security of the Ledidi production environment are the responsibility of AWS and are covered by their SOC 2 report **(6.17)**. The majority of Ledidi's workforce works remotely. Physical security controls are deemed not applicable for Ledidi as client data and/or ePHI is housed entirely within AWS.

Ledidi's acceptable use policy, which all new hires must review and acknowledge, provides the requirements for handling documents, physical media, and storage devices along with the information classification and handling scheme **(6.18)**. The policy describes the handling of physical documents, including storing such documents in locked cabinets/drawers when not needed or outside of work hours. The policy also states that documents containing health and personal data shall not be printed. Ledidi operates on a clear desk, clear screen policy.

Virtual Private Cloud: Virtual private cloud (VPC) rules are configured to block unauthorized traffic into the network **(6.19)**. Access to modify VPC rules is restricted to authorized individuals **(6.20)**.

Transmission Encryption: All data transfers between users and the Ledidi system are secured using TLS and industry standard encryption **(6.21)**.

Removable Media: Ledidi has taken measures to restrict the usage of removable media to help mitigate both the risk of data loss as well as the risk of malware being introduced onto Ledidi systems. The use of portable devices or removable media is governed by the acceptable use policy **(6.22)**.

Hardware and Data Disposal: Ledidi's acceptable use policy describes the configuration requirements for Ledidi managed and BYOD (bring your own device) devices and the deletion and cleansing or destruction of devices when no longer used for Ledidi purposes **(6.23)**. Ledidi's data retention and deletion procedure defines specific requirements for the retention and disposal of the different types of data Ledidi may possess including PHI **(6.24)**. The data retention is broken into type of data and purpose of such data. This includes employee information, company information, business agreements and supporting documentation, customer content, and data that has been prepared and shared with a data subject.

System Operations

Incident Response Program: Ledidi has a documented incident procedure which establishes the procedures to be undertaken in response to information security incidents **(7.1)**. The incident procedure has been communicated to appropriate personnel and includes the following:

- Definition of an event
- Roles and responsibilities
- Steps to analyze, document, and remediate the identified incident
- Incident severity identification and classification
- Communications protocols
- A retrospective analysis to determine the root cause and implement incident response enhancements

The incident procedure is updated annually, and more frequently based upon incident outcomes and lessons learned, as appropriate **(7.2)**.

Incident Monitoring and Recordkeeping: Ledidi maintains a record of security incidents **(7.3)**. The incident records include a description of the incident and relevant facts (e.g., information that was disclosed), mitigations, risk assessment, and outcomes.

Notification in the Case of Breach: Ledidi's policies and procedures related to breach notification are consistent with the HIPAA Breach Notification Rule. In the event of a breach, Ledidi is required to notify each client affected by the breach **(7.4)**. Business associate agreements with service providers and contractors obligates such organizations to report breaches, if any, to Ledidi in a timely manner **(7.5)**. The data processing agreements Ledidi holds with data controllers requires Ledidi to notify the data controller of any potential personal data breaches **(7.6)**.

Complementary User Entity Controls: *User entities are responsible for assessing whether significant harm occurred in a breach and bear the burden of demonstrating through recordkeeping that all required notifications were made, if warranted, within timing constraints and without unreasonable delay.*

Complementary User Entity Controls: *User entities are responsible for breach notification to individuals, the media, and the Secretary of the U.S. Department of Health and Human Services. Ledidi's responsibility is to report breaches to their user entities.*

Complementary User Entity Controls: *User entities are responsible for coordinating with Ledidi to comply with law enforcement delay requirements of the HIPAA breach notification rule.*

Complementary User Entity Controls: *It is the responsibility of user entities to comply with the HIPAA Security Rule's requirements by obtaining Ledidi's signature on their business associate agreement.*

Workstation Antivirus and Patching: The Company's policies and procedures provide guidance to its personnel concerning the physical safeguarding of workstations with access to the IT environment and information relevant to HIPAA requirements for both company managed and BYOD devices **(7.7)**. The guidance applies to devices such as Windows or MacBook laptops, tablets, or other electronic devices (e.g., fixed workstation, portable workstation/laptop computer, tablet computer, smartphone, etc.) and to locations such as office, home, public place, etc. The guidance also includes access to physical and logical information and data subject to HIPAA requirements. User workstations are required to maintain current patching and operating systems and have antimalware software installed **(7.8)**.

Monitoring of Servers: Ledidi subscribes to AWS' automatic server maintenance and patching service where AWS provides notice to its subscribers of maintenance actions needing to be performed. AWS will automatically perform the described maintenance activity after a defined period of time.

Backups: Ledidi has documented a backup policy that describes how often service and client data are backed up **(7.9)**. All original customer data on Ledidi's infrastructure must be backed up. Database backups are automatically performed hourly and daily, depending upon the data **(7.10)**. Backups are stored within AWS. A backup of the Ledidi database is restored at least annually so that restore operations are executed smoothly, if needed **(7.11)**.

Disaster Recovery Policy: Ledidi has created a business continuity plan to define the organization's procedures to recover IT infrastructure and IT services in the case of an outage or other disruptive incident **(7.12)**.

The following goals have been established for the plan:

1. **High availability:** Provide for the capability and processes so that a business has access to applications regardless of local failures.
2. **Continuous operations:** Safeguard the ability to keep things running during a disruption, as well as during planned outages such as scheduled backups or planned maintenance.
3. **Disaster recovery:** Establish a way to recover a data center at a different site if a disaster destroys the primary site or otherwise renders it inoperable.

Detailed steps and contacts are defined in the plan to provide direction regarding steps to take in the case of a disaster. Ledidi performs a test of the business continuity plan on an annual basis **(7.13).** Various scenarios are tested to determine Ledidi's ability to address each scenario.

Change Management

An effective system development and maintenance process is critical to the availability and integrity of Ledidi's system. The Ledidi Core platform is a proprietary and in-house developed system where custom changes are often necessary to enhance system functionality. Ledidi follows a defined development operating procedure for making changes to the system used to support the services provided to its clients **(8.1)**. Ledidi's development operating procedure describes how changes to the Ledidi system are proposed, reviewed, deployed, and managed. The change management procedure covers all changes made to the Ledidi software, regardless of their size, scope, or potential impact.

A request for a change can come internally from management or Ledidi personnel or externally from clients. A project management tool is used to prioritize, assign the task to team members, and track which changes are authorized for development **(8.2)**. Once assigned, an engineer develops the change and then oversees any needed testing or peer reviews. Engineering uses a software development platform to manage and record activities related to the change management process **(8.3)**. The tool enforces version control and is used to document control points within the change management process. Engineers work on the changes in the development environment. Ledidi maintains separate development, test, and production environments internally **(8.4)**. Part of the change management process involves automated code testing, which includes code security vulnerability checks. Automated testing is run for each change taking place with any errors needing to be remediated prior to moving the change to the next stage of the cycle **(8.5)**.

Once a change is ready for deployment to production, the assigned engineer submits the change's pull request for review, testing, and approval to release the change to production **(8.6)**. Branch protection rules have been configured to require review and approval of the change in order to be released to production **(8.7)**. The quality assurance team has multiple recurring weekly checkpoints to review open items, bug lists, and approve changes for release **(8.8)**.

Authorization to Implement Changes: Ledidi restricts the ability to implement changes into the production environment to only those individuals who require the ability to implement changes as part of their job function **(8.9)**.

Communication of Changes: Changes and enhancements impacting the functionality of the Ledidi software are communicated internally to employees and externally to system users as necessary **(8.10)**.

Risk Mitigation

New Suppliers: Ledidi has a supplier management procedure document that is followed for onboarding new suppliers **(9.1)**. Any suppliers that are key to Ledidi core services are required to be reviewed to validate

conformance of established information security requirements. An inventory of suppliers is maintained that includes the services provided and general compliance information **(9.2)**.

Supplier Risk Assessments: Ledidi understands that risks exist when engaging in business relationships and as a result, considers those risks that could potentially affect Ledidi's ability to meet its internal and external business objectives. See the preceding *Risk Assessment* section for additional information on Ledidi's risk assessment process.

Subservice Providers Monitoring: Ledidi uses a number of suppliers to assist with Ledidi's business needs including security and infrastructure through the services these suppliers provide. Ledidi completes an annual review of key suppliers that includes obtaining and reviewing the supplier's SOC examination **(9.3)**. Ledidi documents the results of the review and includes the review of the complementary subservice organization controls included in the supplier SOC reports **(9.4)**.

(The remainder of this page is left blank intentionally.)

Complementary Subservice Organizations Controls (CSOC)

Ledidi's controls related to the Ledidi core services cover only a portion of the overall internal control for each user entity of Ledidi. It is not feasible for the HIPAA requirements related to the Ledidi core services to be achieved solely by Ledidi. Therefore, each user entity's internal controls must be evaluated in conjunction with Ledidi's controls and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations, described as follows:

	AWS Complementary Subservice Organization Controls	**Related HIPAA Requirements**
1.	The subservice organization is responsible for providing the physical security controls protecting the production servers from unauthorized access.	§ 164.310(a)(1) § 164.310(a)(2)(i)-(iv)
2.	The subservice organization is responsible for providing the environmental controls protecting the production servers.	§ 164.308(a)(1)(ii)(D) § 164.308(a)(6)(i)-(ii) § 164.310(a)(2)(iv)
3.	The subservice organization is responsible for maintaining the availability of the hosted environments 24/7/365.	§ 164.308(a)(5)(ii)(B) § 164.308(a)(7)(i) § 164.308(a)(7)(ii)(A)-(E)
4.	The subservice organization is responsible for managing and resolving incidents and problems reported by Ledidi in a timely manner.	§ 164.308(a)(6)(i) § 164.308(a)(7)(i)

(The remainder of this page is left blank intentionally.)

Ledidi's Complementary User Entity Controls (CUEC)

The Ledidi core services provided by Ledidi for user entities and the controls at Ledidi cover only a portion of the user entity's overall system of internal control. It is not feasible for the HIPAA requirements related to the Ledidi core services to be achieved solely by Ledidi. Therefore, each user entity's internal control must be evaluated in conjunction with Ledidi's controls and the related tests and results described in *Section IV – Independent Service Auditor's Description of Tests of Controls and Results* of this report, taking into account the related complementary user entity controls identified under each area, where applicable.

This section highlights additional control activities that Ledidi believes should be considered and/or present at each user entity. Each user entity must evaluate its own system of internal control to determine if the following controls are in place. User auditors should consider whether the following controls, including all the HIPAA Security and Breach Notification Rules noted in *Section V – HIPAA Requirements and Controls*, have been placed in operation at user organizations. This list is not intended to be, and is not a complete listing of, the controls that provide a basis for the achievement of the HIPAA requirements.

	Complementary User Entity Controls	**Related HIPAA Requirements**
1.	User entities are responsible for executing any required contractual obligations per their regional regulations and/or requirements.	§ 164.314(a)(1)(i)
2.	User entities are responsible for provisioning and deprovisioning user access to authorized individuals according to the principle of least privilege.	§ 164.308(a)(3)(ii)(B) § 164.308(a)(3)(ii)(C) § 164.308(a)(4)(i)
3.	User entities are responsible for periodically reviewing user access and access permissions to determine whether access is limited to appropriate personnel.	§ 164.308(a)(1)(ii)(D)
4.	User entities are responsible for configuring strong password complexity requirements when using their own authentication method into the Ledidi environment.	§ 164.308(a)(5)(ii)(D)
5.	User entities are responsible for configuring multifactor authentication when using their own authentication method into the Ledidi environment.	§ 164.308(a)(5)(ii)(D)

	Complementary User Entity Controls	Related HIPAA Requirements
6.	User entities are responsible for assessing whether significant harm occurred in a breach and bear the burden of demonstrating through recordkeeping that all required notifications were made, if warranted, within timing constraints and without unreasonable delay.	§ 164.404(a)(1)-(2)
7.	User entities are responsible for breach notification to individuals, the media, and the Secretary of the U.S. Department of Health and Human Services. Ledidi's responsibility is to report breaches to their user entities.	§ 164.404(b) § 164.404(c) (1)-(2) § 164.404(d)(1)-(3) § 164.406(a)-(c) § 164.408(a)-(c)
8.	User entities are responsible for coordinating with Ledidi to comply with law enforcement delay requirements of the HIPAA breach notification rule.	§ 164.412 § 164.414(a)-(b)
9.	It is the responsibility of user entities to comply with the HIPAA Security Rule's requirements by obtaining Ledidi's signature on their business associate agreement.	§ 164.410(a)(1)-(2)

(The remainder of this page is left blank intentionally.)

Section IV – Independent Service Auditor's Description of Tests of Controls and Results

Purpose and Objective of the Independent Auditor's Examination

This report on controls placed in operation is intended to provide users of the report with information sufficient to obtain an understanding of Ledidi's compliance activities relevant to the HIPAA requirements described in Section V of this report. This report, when coupled with an understanding of the internal controls in place at each client, is intended to assist in the assessment of the total internal control surrounding the Ledidi core services provided by Ledidi.

Our examination was limited to those controls performed at Ledidi's Oslo, Norway, location. It is each stakeholder's responsibility to evaluate this information in relation to the internal controls in place at each client to obtain an overall understanding of the internal controls and assess control risk. The portion of controls provided by each client and Ledidi must be evaluated together. If effective control activities are not in place at the client, Ledidi's controls may not compensate for such weaknesses.

Our examination included inquiries of appropriate management, supervisory, and staff personnel; inspection of documents and records; observation of activities and operations; and tests of controls surrounding Ledidi's core services. Our tests of controls were performed as of April 30, 2025 and were applied to those controls specified by Ledidi in Sections III and IV of this report.

The description of controls is the responsibility of Ledidi's management. Our responsibility is to express an opinion that the controls are designed with sufficient effectiveness to provide reasonable, but not absolute, assurance that the HIPAA requirements, specified by the U.S. Department of Health and Human Services (HHS), were achieved as of April 30, 2025.

Any exceptions noted by Linford & Company LLP regarding the design of the controls identified to achieve the specified requirements or the level of compliance with the controls are presented in this section under the caption, "Results of Testing." Exceptions identified herein are not necessarily weaknesses in the total system of internal control at Ledidi, as this determination can only be made after consideration of controls in place at each client. Complementary user entity controls that should be exercised by clients in order to complement the controls of Ledidi to attain the HIPAA requirements are presented in Section III when considered applicable.

Overview of the Internal Control Environment

Entity-Level Controls

Our examination considered the control environment and included inquiry of appropriate management and staff, inspection of documents and records, and observation of activities and operations. Our examination was as of April 30, 2025 and was applied to those controls specified by management in Sections III and IV of this report.

The control environment represents the collective effect of various elements in establishing, enhancing, or mitigating the effectiveness of specified controls. In addition to our review of the controls placed into operation, our procedures included tests of the relevant elements of Ledidi's control environment, including Ledidi's organizational structure and management control methods.

Our evaluation of the control environment included the following procedures, to the extent necessary:

- ✓ *Inspected* Ledidi's organizational structure, including the segregation of functional responsibilities, personnel policies, and other policies and procedures.
- ✓ *Inquired* through discussion with management personnel responsible for developing, monitoring, and enforcing controls.
- ✓ *Observed* personnel in the performance of their assigned duties.

No exceptions were noted in entity-level testing.

* * * * *

The results of these procedures were considered in planning the nature, timing, and extent of evaluation procedures around the design of controls.

Controls Specified by Ledidi, Testing Procedures, and Results of Tests

The following tables include a description of the control activities, testing procedures performed, and results of tests. Ledidi management specified the control activities and the HHS specified the HIPAA requirements in *Section V – HIPAA Requirements and Controls*.

HIPAA Security and Breach Notification Controls

Control Environment

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
1.1	A board of directors, consisting of internal and external individuals, exercises oversight of Ledidi's strategic direction, operational performance, and internal control.	*Inspected* the board of directors listing and meeting minutes and noted that the board of directors included both internal and external members For a sample board meeting, *inspected* the meeting minutes and noted that the board met at least quarterly to discuss items related to Ledidi.	No exceptions noted. No exceptions noted.
1.2	The executive management team meets on a weekly basis.	For a sample management meeting, *inspected* the meeting invite and minutes and noted that the meeting occurred weekly and included members of executive management.	No exceptions noted.
1.3	Ledidi's LICS applies to all full-time, part-time, and contractor staff and includes the following sections: goals and annual plan, security, code of conduct, disciplinary process, and reporting violations.	*Inspected* Ledidi's code of conduct and noted that it included expected employee and contractor behaviors as noted within the control.	No exceptions noted.

Control Environment (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
1.4	Ledidi has established an internal compliance function and supporting tools which monitor the Ledidi control environment and alerts management when internal control and security issues arise.	*Inspected* an audit report and noted that an audit was performed on Ledidi's internal control environment. *Inspected* the internal monitoring tools and noted that management used the tools to alert when security issues arose.	No exceptions noted. No exceptions noted.
1.5	Ledidi's organizational structure defines authorities across the Company to facilitate information flow and establish responsibilities.	*Inspected* Ledidi's organizational structure and noted that it defined responsibilities and lines of authority throughout the organization.	No exceptions noted.
1.6	To increase the operational effectiveness of employees within this structure, every position has a job description so that individuals understand their responsibilities.	For a sample job title, *inspected* the documented job description for the position and noted that it reflected the employee's responsibilities.	No exceptions noted.
1.7	The HIPAA Security Officer is responsible for the security of Ledidi's systems including security relating to HIPAA compliance.	*Inspected* the HIPAA Security Officer's job description and noted that the role of Security Officer had been assigned and was responsible for the security of Ledidi's systems, including security relating to HIPAA compliance.	No exceptions noted.

Control Environment (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
1.8	Applicants for full-time employment at Ledidi are required to complete a successful reference check as part of the terms of their employment.	For a sample recent new hire, *inspected* the onboarding checklist and noted that a reference check was completed.	No exceptions noted.
1.9	As part of the hiring process, applicants are required to sign an employee contract that contains a confidentiality agreement.	For a sample recent new hire, *observed* the offer letter and confidentiality agreement and noted that both documents were signed by the new hire prior to the individual's start date.	No exceptions noted.
1.10	An onboarding checklist is completed to monitor completion of employment documentation and acknowledgment of Ledidi's LICS and assigned policies.	For a sample recent new hire, *inspected* the policy acknowledgement and noted that the new hire acknowledged the required policies and procedures as part of onboarding.	No exceptions noted.
1.11	New hires are required to complete Ledidi security awareness training and HIPAA training and sign the HES Declaration at the start of their position.	For a sample recent new hire, *inspected* training logs and noted that the new hire completed security awareness and HIPAA training as part of onboarding.	No exceptions noted.
1.12	Employee performance and feedback reviews are performed at least annually.	For a sample employee, *inspected* performance review documentation and noted that the performance review was performed within the past year.	No exceptions noted.

Information and Communication

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
2.1	Ledidi maintains policies to communicate HIPAA security and privacy responsibilities to Ledidi personnel.	*Inspected* the Ledidi internal privacy and acceptable use policy and noted that Ledidi communicated security and privacy responsibilities to Ledidi personnel.	No exceptions noted.
2.2	Ledidi uses an internal communication tool to distribute policies and periodic security reminders to employees including responsibilities related to security.	*Inspected* Ledidi's internal communication tool and noted that it was used to distribute policies. *Inspected* security communication to employees and noted that security reminders were conducted.	No exceptions noted. No exceptions noted.
2.3	Ledidi management provides annual security awareness training and HIPAA training for all employees that covers information security, data protection, and confidentiality of client information.	*Inspected* training materials and noted that Ledidi provided security awareness training, privacy, and HIPAA training on an annual basis covering information security, data protection, and confidentiality. *Inspected* the security awareness training and HIPAA training records for a sample employee and noted that the employee completed the trainings within the past year.	No exceptions noted. No exceptions noted.
2.4	Ledidi has created a high-level overview of the Ledidi system used to describe the services provided to the clients that Ledidi serves.	*Inspected* the Ledidi product and IT-architecture information on the Ledidi website and noted that a high-level overview of the Ledidi system was available to clients that Ledidi serves.	No exceptions noted.

Information and Communication (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
2.5	Ledidi and its clients' responsibilities and commitments regarding the acceptable use of the Ledidi system and PHI, as applicable are included within the Ledidi Enterprise Agreement and Terms of Service which clients must agree to before using the Ledidi software.	*Inspected* the Ledidi Enterprise Agreement and Terms of Service and noted that they included Ledidi's clients' responsibilities and commitments regarding the acceptable use of the Ledidi system and PHI.	No exceptions noted.
2.6	For any service provider handling PHI on behalf of Ledidi, a BAA is also required to be executed.	For the only service provider, *inspected* the BAA and noted that it provided the terms for the business associate and covered entity regarding the handling of PHI of the covered entity by the business associate.	No exceptions noted.
2.7	Ledidi has provided methods to clients and employees to report failures, incidents, concerns, or other complaints related to the services or systems provided by Ledidi in the event there are problems.	*Inspected* the Ledidi core services and noted that methods were provided to clients to report issues and other concerns to the Company. *Inspected* internal policies and noted that employees were provided with information on how to report failures, incidents, concerns, or other complaints.	No exceptions noted. No exceptions noted.

Risk Assessment

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
3.1	Ledidi's risk assessment procedure describes the processes Ledidi has in place to identify new business and technical risks and how to achieve the desired level of risk.	*Inspected* the risk assessment procedure and noted that Ledidi had a process in place to identify and mitigate new business and technical risks.	No exceptions noted.
3.2	The policy is made available to all employees through the Company's policy depository.	*Inspected* the policy repository on the internal compliance portal and noted that Ledidi's risk assessment procedure was available to employees on the compliance management portal.	No exceptions noted.
3.3	Annually, the risks identified are formally documented in a risk assessment matrix.	*Inspected* the risk assessment matrix and noted that the risk assessment documented identified risk scenarios.	No exceptions noted.
3.4	Risk owners work with the Compliance Officer in the development of a risk treatment plan per risk assessment performed and the risk assessment is reviewed by Ledidi management.	*Inspected* the risk assessment matrix and noted that the risk identification and treatment plan were the joint responsibility of the Compliance Officer and department heads for the respective areas covered.	No exceptions noted.
3.5	The supplier management procedures provide a framework for managing the life cycle of supplier relationships.	*Inspected* the vendor management policy and noted that it provided guidance for managing the life cycle of vendor relationships.	No exceptions noted.

Risk Assessment (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
3.6	Ledidi has considered the potential for fraud when assessing risks to the achievement of objectives.	Through *inquiries* of Ledidi management, determined that the potential for fraud was addressed through internal processes implemented within the organization.	No exceptions noted.
3.7	Ledidi's risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.	Through *inquiries* of Ledidi management, noted that Ledidi considered changes to the regulatory, economic, and physical environment in which the entity operates.	No exceptions noted.

Monitoring Activities

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
4.1	Ledidi uses AWS monitoring tools to monitor application health and the monitoring tool alerts system administrators when the application is not operating within defined boundaries.	*Inspected* the monitoring tool and noted that Ledidi monitored application health and that the monitoring tool sent alerts when the application was not operating within defined boundaries.	No exceptions noted.
4.2	Ledidi logs authentication, availability, and error events and uses tools for infrastructure monitoring.	*Inspected* monitoring tools and noted that Ledidi monitored the infrastructure as well as logged authentication, availability, and error events.	No exceptions noted.
4.3	The client-submitted tickets are addressed by Ledidi personnel.	*Inspected* a sample ticket submitted by a client and noted that the ticket described the issue identified by the client and the steps taken by Ledidi personnel to address the issue.	No exceptions noted.
4.4	Ledidi has implemented steps within the change management process to test for security vulnerabilities that could impact operations of the Ledidi Core service offering.	For a sample change during the period, *inspected* the change request documentation and noted that the change was automatically tested and was successfully completed prior to the change being deployed to production.	No exceptions noted.
4.5	Ledidi annually has a third-party application penetration test performed and issues identified during the test are remediated, as needed.	*Inspected* the penetration test results and noted that the test was performed during the audit period and identified vulnerabilities were reviewed and addressed as appropriate by Ledidi's management.	No exceptions noted.

Control Activities

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
5.1	Part of this oversight includes the establishment of policies and procedures to manage and direct company activity and to allow for periodic assessments of adherence to the policies and procedures.	*Inspected* the policies and procedures and noted that they provided direction regarding performance of activities including security, privacy, and HIPAA.	No exceptions noted.
5.2	Ledidi's management also segregates responsibilities and duties across the organization to mitigate risks to the services provided to its clients and to the Ledidi Core platform.	*Inspected* the Ledidi organizational chart, system configurations, and role assignments and determined that responsibilities and duties were segregated within the organization and within the Ledidi environment.	No exceptions noted.
5.3	Ledidi has established a compliance program for management and monitoring of key practices and control points with key components of compliance, HIPAA, and security.	*Inspected* the internal compliance program and noted that management maintained the program and reviewed control activities. *Inspected* compliance reporting of activity performed during the audit period and noted it detailed the different compliance activities performed as well as outcomes of these activities.	No exceptions noted. No exceptions noted.
5.4	The compliance program includes monitoring of key activity and tracking of activity through a non-conformity register.	*Inspected* the non-conformity register and a sample report for an item listed on the non-conformity register and noted that reported items were tracked through completion.	No exceptions noted.

Control Activities (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
5.5	Meetings are held to review identified company activities, current status, and remediation activities.	*Inspected* invitations for meetings held to discuss product and development activity and noted that meetings were held regularly with relevant team members to address the topics under the responsibility of the meeting attendees.	No exceptions noted.
5.6	Results of these compliance activities are presented at company management meetings.	*Inspected* a sample management review report and noted that it detailed status of risk assessment activities including non-conformity activities.	No exceptions noted.

Information Security

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
6.1	Ledidi's system access procedures document the requirements for registering and authorizing employees and contractors prior to being issued system credentials and granted the ability to access the system.	*Inspected* Ledidi's system access procedures and noted that the procedures specified requirements for registering and authorizing employees prior to being issued system credentials and granted the ability to access the system.	No exceptions noted.
6.2	Ledidi employees are granted access to Ledidi systems according to their role and/or team.	*Inspected* Ledidi's onboarding process document and noted that it specified that new hires were only granted access to systems according to their role and/or team. Through *inspection* of the access breakdown matrix, noted that users were assigned authorities based on their type of role and/or team.	No exceptions noted. No exceptions noted.
6.3	Access is provisioned by the security officer based on notification received from the CEO authorizing such access.	For a sample recent new hire, *inspected* the email authorizing access and the onboarding checklist and determined that access was authorized and actions taken were documented.	No exceptions noted.
6.4	In addition, Ledidi employees and contractors must accept the Company's acceptable use policy upon being hired.	For a sample recent new hire, *inspected* policy acknowledgments within the internal compliance tool and noted that the new hire accepted the acceptable use policy.	No exceptions noted.

Information Security (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
6.5	When an employee or contractor is terminated, the Security team revokes production access upon termination.	For a sample individual recently terminated, *inspected* offboarding documentation and noted that system access was revoked within three business days of the termination date.	No exceptions noted.
6.6	On a semi-annual basis, the system owners conduct a user appropriateness review of access to Ledidi resources to validate internal user access is commensurate with job responsibilities.	*Inspected* a sample management review report and noted that the security performance review was conducted including identification and remediation of any non-conformities.	No exceptions noted.
6.7	Administrator-level access privileges to the production environment are restricted to only those individuals who require such access to perform their respective job functions.	For a sample user with administrator access to the production infrastructure, *inspected* the HR organization chart and noted that access was appropriate to the user's job functions and the individual was a current employee or contractor. For a sample user with administrator access to the production infrastructure, *inquired* of Ledidi's management and noted that access was appropriate to the user's job function.	No exceptions noted. No exceptions noted.

Information Security (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
6.8	Password parameters to production systems enforce standards for minimum length and complexity.	*Inspected* the password policy and noted that password protection requirements were documented and defined for Ledidi production systems. *Inspected* password configurations for production systems and noted that strong password settings were enforced.	No exceptions noted. No exceptions noted.
6.9	Remote access to the production infrastructure is limited to authorized individuals and communications are encrypted.	*Inspected* the system configuration and noted that SSH using RSA and a private key was required to log directly onto a server.	No exceptions noted.
6.10	Access to client data within the Ledidi production database by Ledidi employees is restricted to authorized users.	For a sample user with access to client data, *inspected* the HR organization chart and noted that access was appropriate to the user's job functions and the individual was a current employee or contractor. For a sample user with administrator access to the production infrastructure, *inquired* of Ledidi's management and noted that access was appropriate to the users' job function.	No exceptions noted. No exceptions noted.

Information Security (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
6.11	In addition, client users have access to their data only and no other clients' data.	*Observed* a technical demonstration and noted that Ledidi clients may not access other clients' data.	No exceptions noted.
6.12	Client data within Ledidi's production databases is encrypted.	*Inspected* database configurations and noted that client data within Ledidi's production databases was encrypted.	No exceptions noted.
6.13	Multifactor authentication is required for access to the production environment.	*Inspected* system configurations and noted that multifactor authentication was required for access to the infrastructure.	No exceptions noted.
6.14	The Company's policies and procedures provide guidance to its personnel concerning the physical safeguarding of workstations with access to the IT environment and information relevant to HIPAA requirements for company devices.	*Inspected* Ledidi's acceptable use policy and noted that it specified measures to physically safeguard access to workstations.	No exceptions noted.
6.15	User workstations are required to be encrypted, maintain current patching and operating systems, have antimalware software installed, and configured to automatically lock after five minutes of inactivity.	For a sample employee, *inspected* their workstation's configurations and determined that the workstation had encryption enabled, was on a supported operating system level, had antimalware installed, and was configured to automatically lock after five minutes of inactivity.	No exceptions noted.

Information Security (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
6.16	Only authorized Ledidi personnel have a keycard to the Ledidi office.	For a sample individual defined in the building physical access listing, *inspected* the Ledidi personnel listing and noted that access was appropriate. For a sample individual recently terminated, *inspected* the physical access listing to the Ledidi office and noted that keycard was not issued to the individual.	No exceptions noted. No exceptions noted.
6.17	Physical and environmental security of the Ledidi production environment are the responsibility of AWS and are covered by their SOC 2 report.	*Inspected* the annual vendor review that Ledidi completed for AWS and noted that the subservice organization had been monitored during the examination period and that Ledidi documented the review of the AWS SOC report.	No exceptions noted.
6.18	Ledidi's acceptable use policy, which all new hires must review and acknowledge, provides the requirements for handling documents, physical media, and storage devices along with the information classification and handling scheme.	*Inspected* the acceptable use policy and noted that it provided the requirements for handling documents, physical media, and storage devices along with the information classification and handling scheme.	No exceptions noted.
6.19	VPC rules are configured to block unauthorized traffic into the network.	*Inspected* the VPC rules and noted that they were configured to block unauthorized internet traffic.	No exceptions noted.

Information Security (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
6.20	Access to modify VPC rules is restricted to authorized individuals.	For a sample user with access to modify VPC rules, *inspected* the employee listing and noted that access was commensurate with the user's job function. For a sample user with access to modify VPC rules, *inquired* of Ledidi's management and determined that the user's access was appropriate.	No exceptions noted. No exceptions noted.
6.21	All data transfers between users and the Ledidi system are secured using TLS and industry standard encryption.	*Inspected* website security settings and noted that data transfers between users and the Ledidi system used TLS and industry standard encryption.	No exceptions noted.
6.22	The use of portable devices or removable media is governed by the acceptable use policy.	*Inspected* the acceptable use policy and noted that the usage of portable devices or removable media was allowed in accordance with the information classification and handling scheme, which provides the classification level of data handled by Ledidi and the level of protection to be provided for each data classification.	No exceptions noted.

Information Security (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
6.23	Ledidi's acceptable use policy describes the configuration requirements for Ledidi managed and BYOD devices and the deletion and cleansing or destruction of devices when no longer used for Ledidi purposes.	*Inspected* the acceptable use policy and noted that it addressed the configuration requirements of Ledidi managed and BYOD devices and the deletion and cleansing or destruction of devices when no longer used for Ledidi purposes.	No exceptions noted.
6.24	Ledidi's data retention and deletion procedure defines specific requirements for the retention and disposal of the different types of data Ledidi may possess including PHI.	*Inspected* the data retention and deletion procedure and noted that client data was required to be deleted within one week of the deletion request.	No exceptions noted.

System Operations

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
7.1	Ledidi has a documented incident procedure which establishes the procedures to be undertaken in response to information security incidents.	*Inspected* the incident procedure and noted that it detailed procedures for incident response in the event of a security incident.	No exceptions noted.
7.2	The incident procedure is updated annually, and more frequently based upon incident outcomes and lessons learned, as appropriate.	*Inspected* the incident procedure and noted that it was updated and approved within the last year.	No exceptions noted.
7.3	Ledidi maintains a record of security incidents.	For a sample security incident during the period, *inspected* Ledidi's incident tracking documentation and noted that Ledidi maintained a record of the security incident and followed the incident through to resolution. Noted through *inquiries* of management that there were no incidents that occurred that required usage of the incident response procedure.	No exceptions noted. No exceptions noted.
7.4	In the event of a breach, Ledidi is required to notify each client affected by the breach.	*Inspected* Ledidi's incident and communication procedures and noted that they included requirements to notify affected clients. *Inquired* of management and noted that no ePHI breaches occurred during the exam period.	No exceptions noted. No exceptions noted.

System Operations (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
7.5	Business associate agreements with service providers and contractors obligates such organizations to report breaches, if any, to Ledidi in a timely manner.	*Inspected* the business associate agreement for applicable service providers and noted that they obligated the service provider to report breaches to Ledidi in a timely manner.	No exceptions noted.
7.6	The data processing agreements Ledidi holds with data controllers requires Ledidi to notify the data controller of any potential personal data breaches.	*Inspected* the data processing agreement and noted that it required Ledidi to notify the controller of a personal data breach notification affecting the controller's personal data.	No exceptions noted.
7.7	The Company's policies and procedures provide guidance to its personnel concerning the physical safeguarding of workstations with access to the IT environment and information relevant to HIPAA requirements for both company managed and BYOD devices.	*Inspected* Ledidi's acceptable use policy and noted that it specified measures to physically safeguard access to workstations.	No exceptions noted.
7.8	User workstations are required to maintain current patching and operating systems and have antimalware software installed.	For a sample employee, *inspected* workstation configurations and determined that the workstation was on a supported operating system level and had antimalware installed.	No exceptions noted.

System Operations (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
7.9	Ledidi has documented a backup policy that describes how often service and client data are backed up.	*Inspected* the backup policy and noted that the frequency for backups had been documented.	No exceptions noted.
7.10	Database backups are automatically performed hourly and daily, depending upon the data.	*Inspected* backup configurations and backup logs and noted that daily backups were scheduled and performed within the cloud infrastructure.	No exceptions noted.
7.11	A backup of the Ledidi database is restored at least annually so that restore operations are executed smoothly, if needed.	*Inspected* a Ledidi database and noted that the database backup was successfully restored during the audit period.	No exceptions noted.
7.12	Ledidi has created a business continuity plan to define the organization's procedures to recover IT infrastructure and IT services in the case of an outage or other disruptive incident.	*Inspected* Ledidi's business continuity plan and noted that it addressed its plan for recovering form outages or disruption of services.	No exceptions noted.
7.13	Ledidi performs a test of the business continuity plan on an annual basis.	I*nspected* business continuity exercises performed during the period and noted that the exercises tested various scenarios that could occur at Ledidi to determine Ledidi's ability to address such scenarios should they arise.	No exceptions noted.

Change Management

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Tests
8.1	Ledidi follows a defined development operating procedure for making changes to the system used to support the services provided to its clients.	*Inspected* the documented development operating procedure and noted that Ledidi followed a defined development process for making changes to the system.	No exceptions noted.
8.2	A project management tool is used to prioritize, assign the task to team members, and track which changes are authorized for development.	*Inspected* documentation from the project management tool and noted that Ledidi used the tool to prioritize, assign tasks, and track changes to Ledidi systems.	No exceptions noted.
8.3	Engineering uses a software development platform to manage and record activities related to the change management process.	For a sample change, *inspected* the change request documentation and noted that Ledidi used a development tool to manage and record the activities related to the change management process.	No exceptions noted.
8.4	Ledidi maintains separate development, test, and production environments internally.	*Inspected* the environments at Ledidi and noted that there were separate environments for developing, testing, and production for implementing changes.	No exceptions noted.

Change Management (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
8.5	Automated testing is run for each change taking place with any errors needing to be remediated prior to moving the change to the next stage of the cycle.	For a sample change, *inspected* the change request documentation and noted that the change was automatically tested and successfully completed prior to the change being deployed to production.	No exceptions noted.
8.6	Once a change is ready for deployment to production, the assigned engineer submits the change's pull request for review, testing, and approval to release the change to production.	For a sample change, *inspected* the change request documentation and noted that the change was reviewed, approved, and tested prior to being deployed to production.	No exceptions noted.
8.7	Branch protection rules have been configured to require review and approval of the change in order to be released to production.	*Inspected* the branch protection rules and noted that the rules were configured to require a review and approval prior to merging the change into the master branch.	No exceptions noted.
8.8	The quality assurance team has multiple recurring weekly checkpoints to review open items, bug lists, and approve changes for release.	*Inspected* the recurring meeting invites for the quality assurance team and noted that multiple milestones were scheduled weekly to review and approve changes to the production environment prior to release.	No exceptions noted.

Change Management (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
8.9	Ledidi restricts the ability to implement changes into the production environment to only those individuals who require the ability to implement changes as part of their job function.	For a sample user with the ability to implement changes into the production environment, *inspected* the employee information and noted that the individual was a current employee and access was appropriate based on the job role. For a sample user with the ability to implement changes into the production environment, *inquired* of management and noted that the individual was a current employee and access was appropriate based on the job role. *Inspected* branch protection rules and noted that rules were in place requiring changes to be approved prior to production deployment.	No exceptions noted. No exceptions noted. No exceptions noted.
8.10	Changes and enhancements impacting the functionality of the Ledidi software are communicated internally to employees and externally to system users as necessary.	*Inspected* sample internal and external communications and noted that they provided information on changes and enhancements to the Ledidi Core platform.	No exceptions noted.

Risk Mitigation

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Tests
9.1	Ledidi has a supplier management procedure document that is followed for onboarding new suppliers.	*Inspected* the supplier management procedure and associated process document for onboarding of new vendors and noted that a risk assessment and compliance checks were performed as part of the vendor onboarding process.	No exceptions noted.
9.2	An inventory of suppliers is maintained that includes the services provided and general compliance information.	*Inspected* the documented supplier inventory and noted that Ledidi maintains an inventory of suppliers that provide infrastructure and security services.	No exceptions noted.
9.3	Ledidi completes an annual review of key suppliers that includes obtaining and reviewing the supplier's SOC examination.	*Inspected* the documented review of a subservice provider's SOC report and noted that Ledidi completed a review of the SOC report, including review of the complementary user entity controls defined in the report.	No exceptions noted.
9.4	Ledidi documents the results of the review and includes the review of the complementary subservice organization controls included in the supplier SOC reports.	*Inspected* the documented review of a subservice provider's SOC report and noted that Ledidi monitored the complementary user entity controls included in the vendor's SOC report during the period.	No exceptions noted.

Section V – HIPAA Requirements and Controls

Management is responsible for establishing and maintaining effective controls over its Ledidi core services. The controls are designed to provide reasonable assurance to Ledidi leadership and the board of directors that the below HIPAA requirements are achieved.

In the table following, the columns have these meanings:

HIPAA Requirements – This column contains, for each criterion evaluated, the name and regulatory reference citation. Each criterion sources from a standard or implementation specification of the HIPAA Security Rule, or a requirement from the HIPAA Breach Notification Rule.

R/A –This column signifies whether the criterion is "Required" or "Addressable."

Required – Criteria marked as "R" must be implemented without exception. This applies to all the HIPAA Security Rule *standards*, HIPAA Security Rule *implementation specifications* if they are marked as such, and all of the HIPAA Breach Notification Rule requirements.

Addressable – Criteria marked as "A" must be implemented unless it is not reasonable and appropriate under the circumstances to do so. See the HIPAA Security Rule in the Federal Register for more information on unimplemented or partially implemented addressable implementation specifications.

Requirement(s) – This column contains the text of the criterion (requirement) directly from the regulation.

Ref. – This column contains the reference to the control activities in Section III, *Ledidi's Description of Its Ledidi Core Services*, which are relevant to the achievement of the criterion. This column may also contain "CSOC" (complementary subservice organization control) to signify that the specified subservice organization bears partial responsibility for the requirement. A summary of complementary subservice organization controls is included in Section III of this report.

The purpose of this table is to demonstrate that all HIPAA requirements in scope were assessed and that the control activities described in Section III, *Ledidi's Description of Its Ledidi Core Services*, address all of the HIPAA requirements.

HIPAA Security Rule

Administrative Safeguards

The Administrative Safeguards group addresses the administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information (ePHI) and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.

HIPAA Requirements	R/A	Requirement(s)	Ref.
Security Management Process § 164.308(a)(1)(i) Standard	R	Implement policies and procedures to prevent, detect, contain, and correct security violations.	2.1, 2.3, 7.1-7.4, 6.1
Risk Analysis § 164.308(a)(1)(ii)(A)	R	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the covered entity.	3.1-3.7
Risk Management § 164.308(a)(1)(ii)(B)	R	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Sec. 164.306(a) [Security standards: General rules; (a) General requirements].	6.1-6.23, 9.1-9.4
Sanction Policy § 164.308(a)(1)(ii)(C)	R	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	1.12
Information System Activity Review § 164.308(a)(1)(ii)(D)	R	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	4.1-4.2, 6.6, AWS CSOC, CUEC

HIPAA Requirements	R/A	Requirement(s)	Ref.
Assigned Security Responsibility § 164.308(a)(2) Standard	R	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	1.7
Workforce Security § 164.308(a)(3)(i) Standard	R	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic PHI, 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 PHI.	6.1-6.4, 6.6
Authorization and/or Supervision § 164.308(a)(3)(ii)(A)	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.	2.1, 6.1
Workforce Clearance Procedure § 164.308(a)(3)(ii)(B)	A	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	6.2-6.3, 6.6, CUEC
Termination Procedures § 164.308(a)(3)(ii)(C)	A	Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) [Workforce Clearance Procedures] of this section.	6.5, CUEC
Information Access Management § 164.308(a)(4)(i) Standard	R	Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E [Privacy of Individually Identifiable Health Information] of this part.	6.1-6.3, CUEC

HIPAA Requirements	R/A	Requirement(s)	Ref.
Isolating Healthcare Clearinghouse Function § 164.308(a)(4)(ii)(A)	R	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.	N/A[1]
Access Authorization § 164.308(a)(4)(ii)(B)	A	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.	6.2-6.4
Access Establishment and Modification § 164.308(a)(4)(ii)(C)	A	Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	6.1-6.6
Security Awareness and Training § 164.308(a)(5)(i) Standard	R	Implement a security awareness and training program for all members of its workforce (including management).	1.11, 2.3
Security Reminders § 164.308(a)(5)(ii)(A)	A	Periodic security updates.	2.3
Protection from Malicious Software § 164.308(a)(5)(ii)(B)	A	Procedures for guarding against, detecting, and reporting malicious software.	4.1-4.5, 7.1-7.3, 7.8, AWS CSOC
Log-in Monitoring § 164.308(a)(5)(ii)(C)	A	Procedures for monitoring login attempts and reporting discrepancies.	4.2
Password Management § 164.308(a)(5)(ii)(D)	A	Procedures for creating, changing, and safeguarding passwords.	6.8, CUEC

[1] Ledidi does not perform the activities of a health care clearinghouse or of a group health plan; therefore, the additional requirements related to health care clearinghouses and group health plans are not applicable.

HIPAA Requirements	R/A	Requirement(s)	Ref.
Security Incident Procedures § 164.308(a)(6)(i) Standard	R	Implement policies and procedures to address security incidents.	7.1-7.4, AWS CSOC
Response and Reporting § 164.308(a)(6)(ii)	R	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; and document security incidents and their outcomes.	7.1-7.4, 4.1-4.3, AWS CSOC
Contingency Plan § 164.308(a)(7)(i) Standard	R	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 PHI.	7.1-7.4, 7.12-7.13, AWS CSOC
Data Backup Plan § 164.308(a)(7)(ii)(A)	R	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	7.9-7.11, AWS CSOC
Disaster Recovery Plan § 164.308(a)(7)(ii)(B)	R	Establish (and implement as needed) procedures to restore any loss of data.	7.11, AWS CSOC
Emergency Mode Operation Plan § 164.308(a)(7)(ii)(C)	R	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode.	7.12-7.13, AWS CSOC
Testing and Revision Procedure § 164.308(a)(7)(ii)(D)	A	Implement procedures for periodic testing and revision of contingency plans.	7.9, 7.12-7.13, AWS CSOC
Applications and Data Criticality Analysis § 164.308(a)(7)(ii)(E)	A	Assess the relative criticality of specific applications and data in support of other contingency plan components.	7.12-7.13, AWS CSOC

HIPAA Requirements	R/A	Requirement(s)	Ref.
Evaluation § 164.308(a)(8) Standard	R	Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic PHI, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.	3.3-3.7, 9.1-9.4
Business Associate Contracts and Other Arrangements § 164.308(b)(1) Standard	R	A covered entity, in accordance with 164.306 [Security Standards: General Rules], 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 Sec. 164.314(a) [Business Associate Contracts or Other Arrangements] that the business associate will appropriately safeguard the information.	2.5-2.6
Written Contract or Other Arrangements § 164.308(b)(4)	R	Document the satisfactory assurances required by paragraph (b)(1) [Business Associate Contracts and Other Arrangements] of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a) [Business Associate Contracts or Other Arrangements].	2.5-2.6

Physical Safeguards

The Physical Safeguards group addresses the physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

HIPAA Control Criteria	R/A	Requirement(s)	Ref.
Facility Access Controls § 164.310(a)(1) Standard	R	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.	AWS CSOC
Contingency Operations § 164.310(a)(2)(i)	A	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.	AWS CSOC
Facility Security Plan § 164.310(a)(2)(ii)	A	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	AWS CSOC
Access Control and Validation Procedures § 164.310(a)(2)(iii)	A	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.	AWS CSOC
Maintenance Records § 164.310(a)(2)(iv)	A	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).	AWS CSOC[2]

[2] Ledidi uses a data center facility where all data resides, therefore requirements around physical access are not applicable.

HIPAA Control Criteria	R/A	Requirement(s)	Ref.
Workstation Use § 164.310(b) Standard	R	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 PHI.	2.1, 6.1, 6.14, 6.23
Workstation Security § 164.310(c) Standard	R	Implement physical safeguards for all workstations that access electronic PHI, to restrict access to authorized users.	2.1, 6.14-6.15
Device and Media Controls § 164.310(d)(1) Standard	R	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.	6.22-6.23
Disposal § 164.310(d)(2)(i)	R	Implement policies and procedures to address the final disposition of electronic PHI, and/or the hardware or electronic media on which it is stored.	6.23-6.24
Media Re-use § 164.310(d)(2)(ii)	R	Implement procedures for removal of electronic PHI from electronic media before the media are made available for reuse.	6.23-6.24
Accountability § 164.310(d)(2)(iii)	A	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	6.24
Data Backup and Storage § 164.310(d)(2)(iv)	A	Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	7.9-7.11

Technical Safeguards

The Technical Safeguards group addresses the technologies and the policies and procedures for its use that protect electronic protected health information and control access to it.

HIPAA Control Criteria	R/A	Requirement(s)	Ref.
Access Control § 164.312(a)(1) Standard	R	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) [Information Access Management].	6.1-6.24
Unique User Identification § 164.312(a)(2)(i)	R	Assign a unique name and/or number for identifying and tracking user identity.	6.2, 6.7, 6.9
Emergency Access Procedure § 164.312(a)(2)(ii)	R	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	7.11-7.12
Automatic Logoff § 164.312(a)(2)(iii)	A	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	6.15
Encryption and Decryption § 164.312(a)(2)(iv)	A	Implement a method to encrypt and decrypt electronic protected health information.	6.12, 6.21
Audit Controls § 164.312(b) Standard	R	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	4.1-4.3

HIPAA Control Criteria	R/A	Requirement(s)	Ref.
Integrity § 164.312(c)(1) Standard	R	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	6.1-6.5, 6.10-6.11
Mechanism to Authenticate Electronic Protected Health Information § 164.312(c)(2)	A	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	4.2, 4.4, 4.6
Person or Entity Authentication § 164.312(d) Standard	R	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	4.2, 6.8-6.11
Transmission Security § 164.312(e)(1) Standard	R	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	6.19-6.21
Integrity Controls § 164.312(e)(2)(i)	A	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	6.23-6.24
Encryption § 164.312(e)(2)(ii)	A	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	6.12, 6.20-6.21

Organizational Requirements

The Organizational Requirements group addresses the contractual requirements applicable to covered entities and business associates, as well as the requirements for group health plans.

HIPAA Control Criteria	R/A	Requirement(s)	Ref.
Business Associate Contracts or Other Arrangements § 164.314(a)(1)(i) Standard	R	The contract or other arrangement between the covered entity and its business associate required by § 164.308(b) [Business Associate Contracts and Other Arrangements] must meet the requirements of paragraph (a)(2)(i) [Business Associate Contracts] or (a)(2)(ii) [Other Arrangements] of this section, as applicable.	2.5-2.6, CUEC
Other Arrangements § 164.314(a)(2)(ii)	R	The covered entity is in compliance with paragraph (a)(1) [Business Associate Contracts or Other Arrangements] of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3) [Organization Requirements].	N/A[3]
Business Associate Contracts with Subcontractors § 164.314(a)(2)(iii)	R	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.	2.5-2.6

[3] Ledidi is not a covered entity and does not perform the activities of a group health plan; therefore, the additional requirements related to covered entities and group health plans are not applicable.

HIPAA Control Criteria	R/A	Requirement(s)	Ref.
Requirements for Group Health Plans § 164.314(b)(1) Standard	R	Except when the only electronic PHI 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 PHI created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	N/A[3]
Group Health Plan Implementation Specification § 164.314(b)(2)(i)	R	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 PHI that it creates, receives, maintains, or transmits on behalf of the group health plan.	N/A[3]
Group Health Plan Implementation Specification § 164.314(b)(2)(ii)	R	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.	N/A[3]
Group Health Plan Implementation Specification § 164.314(b)(2)(iii)	R	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.	N/A[3]
Group Health Plan Implementation Specification § 164.314(b)(2)(iv)	R	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.	N/A[3]

Policies and Procedures and Documentation Requirements

The Policies and Procedures and Documentation Requirements group addresses the requirements for formal policies and procedures and the documentation requirements.

HIPAA Control Criteria	R/A	Requirement(s)	Ref.
Policies and Procedures § 164.316(a) Standard	R	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 may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.	1.3, 2.1, 6.1
Documentation § 164.316(b)(1) Standard	R	(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 of the action, activity, or assessment.	2.1, 6.1
Time Limit § 164.316 (b)(2)(i)	R	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.	2.1, 6.1
Availability § 164.316 (b)(2)(ii)	R	Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	2.1, 6.1

HIPAA Control Criteria	R/A	Requirement(s)	Ref.
Updates § 164.316 (b)(2)(iii)	R	Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	2.1, 6.1

HIPAA Breach Notification Rule

Notification to Individuals

HIPAA Control Criteria	R/A	Requirement(s)	Ref.
General Rule § 164.404(a)(1) Standard	R	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.	CUEC
Breaches Treated as Discovered § 164.404(a)(2) Standard	R	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).	CUEC
Timeliness of Notification § 164.404(b)	R	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.	CUEC

HIPAA Control Criteria	R/A	Requirement(s)	Ref.
Content of Notification – Elements § 164.404(c)(1)	R	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 individuals should take to protect themselves from potential harm resulting from the breach; (D) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and (E) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, website, or postal address.	CUEC
Content of Notification – Plain Language Requirement § 164.404(c)(2) Standard	R	The notification required by paragraph (a) of this section shall be written in plain language.	CUEC

HIPAA Control Criteria	R/A	Requirement(s)	Ref.
Methods of Individual Notification – Written Notice § 164.404(d)(1)	R	The notification required by paragraph (a) of this section shall be provided in the following form: (1) *Written notice.* (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 is 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. The notification may be provided in one or more mailings as information is available.	CUEC

HIPAA Control Criteria	R/A	Requirement(s)	Ref.
Methods of Individual Notification – Substitute Notice § 164.404(d)(2)	R	The notification required by paragraph (a) of this section shall be provided in the following form: (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 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 such 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 major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) Include a toll-free phone 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.	CUEC
Methods of Individual Notification – Additional Notice in Urgent Situations § 164.404(d)(3)	R	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.	CUEC

Notification to the Media

HIPAA Control Criteria	R/A	Requirement(s)	Ref.
Notification to the Media § 164.406(a) Standard	R	For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in § 164.404(a)(2), notify prominent media outlets serving the State or jurisdiction. For purposes of this section, State includes American Samoa and the Northern Mariana Islands.	CUEC
Timeliness of Notification § 164.406(b)	R	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.	CUEC
Content of Notification § 164.406(c)	R	The notification required by paragraph (a) of this section shall meet the requirements of § 164.404(c).	CUEC

Notification to the Secretary

HIPAA Control Criteria	R/A	Requirement(s)	Ref.
Notice to the Secretary § 164.408(a) Standard	R	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.	CUEC
Breaches Involving 500 or More Individuals § 164.408(b)	R	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 website.	CUEC

HIPAA Control Criteria	R/A	Requirement(s)	Ref.
Breaches Involving Less Than 500 Individuals § 164.408(c)	R	For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches occurring during the preceding calendar year, in the manner specified on the HHS website.	CUEC

Notification by a Business Associate

HIPAA Control Criteria	R/A	Requirement(s)	Ref.
Notification by a Business Associate § 164.410(a)(1) Standard	R	A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.	7.5-7.6, CUEC
Breaches Treated as Discovered § 164.410(a)(2) Standard	R	For purposes of paragraph (1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).	7.5-7.6, CUEC
Timeliness of Notification § 164.410(b)	R	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.	7.5-7.6

HIPAA Control Criteria	R/A	Requirement(s)	Ref.
Content of Notification § 164.410(c)	R	(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.	7.5-7.6

Law Enforcement Delay

HIPAA Control Criteria	R/A	Requirement(s)	Ref.
Law Enforcement Delay § 164.412 Standard	R	If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.	7.5-7.6, CUEC

Administrative Requirements and Burden of Proof

HIPAA Control Criteria	R/A	Requirement(s)	Ref.
Administrative Requirements § 164.414(a) Standard	R	A covered entity is required to comply with the administrative requirements of § 164.530(b), (d), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart.	7.5-7.6, CUEC
Burden of Proof § 164.414(b) Standard	R	In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosure did not constitute a breach, as defined at § 164.402.	7.5-7.6, CUEC