LAKEMARY
CENTER

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

Security Practices Procedure Manual

Originated: 06/09
Reviewed: 04/10; 07/12; 12/14; 08/18; 10/20; 09/21
Revised: 04/10; 03/17; 10/19; 01/25

Security Practices Procedures Manual

Table of Contents

Title **Page**

Security Practices 3
Access Controls 6
Assigned Security Responsibility 7
Audit Controls 8
Business Associates Contracts and Other Arrangements 9
Contingency Plan 10
Device and Media Controls 11
Evaluation 12
Facility Access Controls 13
Information Access Management 14
Integrity 15
Person or Entity Authentication 16
Security Awareness and Training 17
Security Incident Procedures 19
Security Management 20
Transmission Security 21
Workforce Security 22
Workstation Security 23
Workstation Use 24

Security Practices

Audience

This information applies to all Lakemary staff, volunteers, trainees, interns and any other contractors or agents who access, transmit or maintain Electronic Protected Health Information (EPHI).

Enforcement

All supervisors are responsible for enforcing these procedures. Individuals who violate these procedures will be subject to the appropriate and applicable disciplinary process, up to and including termination or dismissal.

Definitions:

Authorized User: An individual that is granted access to PHI for individuals served through an authorization, IRB waiver or who is performing an activity related to health care operations.

Business Associate: a person or entity who provides certain functions, activities, or services for or to Lakemary, involving the use and/or disclosure of PHI. A business associate is not a Lakemary employee.

Critical Incident File: The Critical Incident File includes all Critical Incident Report Forms completed during an individual’s period of service with Lakemary.

Disclosure: The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Electronic Mail (email): Any message, image form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

Electronic Mail System: Any computer software application that allows electronic mail to be communicated from one computing system to another.

Electronic Protected Health Information: Individually identifiable health information that is transmitted by or maintained in electronic media. It excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act and employment records held by Lakemary in its role as employer.

Minimum Necessary: When using or disclosing PHI or when requesting PHI from another service provider or service organization, Lakemary must limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. Minimum Necessary does not apply in the following circumstances:

1. Disclosures by a service provider for delivery of services (students and trainees are included as health care providers for this purpose),
2. Uses and Disclosures based upon a valid consent to use and disclose PHI for

treatment, payment and health care operations or a valid authorization to use and disclose PHI,

3. Disclosures made to the Secretary of Health and Human Services,
4. Uses and disclosures required by law or directed by agencies responsible for licensure or administrative oversight of Lakemary operations, and
5. Uses and disclosures required by other sections of the HIPAA privacy regulations.
6. Subpoenas and court orders

Payment: Any activities undertaken either by a health plan or by a health care provider to obtain premiums determine or fulfill its responsibility for coverage and the provision of benefits or to obtain or provide reimbursement for the provision of services. These activities include
but are not limited to:

1. Determining eligibility, and adjudication or subrogation of benefit claims,
2. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance, and related health care processing,
3. Review of healthcare services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges,
4. Utilization review activities, including pre-certification and preauthorization services, concurrent and retrospective review of services,
5. Disclosure to consumer reporting agencies of certain PHI relating to collection of premiums or reimbursement.

Record: Any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated.

Service Operations: Any one of the following activities to the extent the activities are related to providing services:

1. Conducting quality assessment and improvement activities, population-based activities relating to improving services or reducing cost of providing services, case management and care coordination, contacting individuals served with information about service alternatives, and related functions that do not involve direct services,
2. Reviewing the competence or qualifications of service providers, evaluating provider performance, conducting training programs in which students or trainees learn under supervision to practice or improve their skills as service providers, accreditation, certification, licensing, or credentialing activities,
3. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing or placing a contract for reinsurance of risk relating to claims for health care,
4. Conducting or arranging for licensure or administrative review, legal services, and auditing functions, including fraud and abuse detection and compliance programs,
5. Business planning and development, such as conducting cost management and planning related analyses related to managing and operating the entity, development or improvement of methods of payment or covered policies,

6. Business management and general administrative activities:

   Management activities related to HIPAA compliance,
   Customer Service,
   Resolution of internal grievances,
   Sale, transfer, merger, or consolidation of covered entities
   Creating de-identified health information or limited data
   set, Fundraising for the benefit of Lakemary.

Treatment (Habilitation Services): The provision, coordination, or management of health care related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to an individual served; or for the referral of an individual served for services from one service provider to another.

Use (with respect to individually identifiable health information): The sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Access Controls

Lakemary will maintain systems to ensure that only those persons who have been granted access can access EPHI. Lakemary will consider the following areas in its access controls: unique user identification, emergency access procedures, automatic logoff and encryption/decryption.

Unique User Identification

Lakemary assigns unique usernames to each employee, including remote users, for identifying and tracking user identities within its systems. Employees are prohibited from sharing usernames with each other or with non-employees.

Remote Access Procedures

Lakemary provides a Virtual Private Network (VPN) for remote access to EPHI. The VPN is available for remote access to EPHI. Additionally, Lakemary maintains multiple locations which may also be used to access EPHI.

Automatic Logoff

Servers at Lakemary are designed to log users off after a specified period of inactivity. The purpose of automatic logoff is to reduce the risk associated with unattended computers.

Encryption/Decryption

Lakemary provides Egress email encryption to each employee to protect EPHI sent via email.

Assigned Security Responsibility

Lakemary has designated the Senior Director of Information Systems as the Information Security Officer under these procedures. The Information Security Officer is responsible for developing and implementing required policies and procedures.

Audit Controls

Lakemary will record and monitor activity in systems that contain EPHI. The following types of audit trails will be employed.

Login attempts and activity
Account management activity
Directory services access
Policy changes
Privilege use and changes
Process tracking
System events

Business Associates Contracts and Other Arrangements

Lakemary will execute a Business Associates Agreement with all business associates with whom Lakemary shares EPHI. Business Associates are those entities who receive EPHI from Lakemary and/or use the EPHI to provide services to Lakemary.

In addition to the assurance provided in the Privacy Practices Business Associates Agreement, the EPHI Business Associates Agreement must include the following:

- The business associate will implement administrative, physical and technical safeguards that reasonably and appropriately protect the EPHI that it creates, receives, maintains, or transmits on behalf of Lakemary,
- The business associate will ensure that any agent, including a subcontractor, to whom it provides such information, agrees to implement reasonable and appropriate safeguards to protect it.
- The business associate will report to Lakemary any security incident of which it becomes aware, and
- The agreement will be terminated by Lakemary if Lakemary determines that the business associate has violated a material term of the contract.

Contingency Plan

Lakemary has established a Disaster Recovery plan for the continuity of operations in the event of an emergency. With respect to the availability of EPHI, the following procedures are established in the event of a security incident or natural disaster: data backup plan, disaster recovery plan, emergency mode operation plan, testing and revisions, and applications and data criticality analysis.

Data Backup Plan **

Data on all Lakemary servers is backed up to disk drives nightly. The backup system incorporates a third-party vendor, NetStandard, Merriam, KS, to test the backups.

Disaster Recovery Plan

In the event that Lakemary's servers are damaged or destroyed, replacement servers would be ordered and in place within one week. Backed up EPHI would be restored to those servers. If faster access to EPHI was required, Lakemary would contract with a local computer service provider (NetStandard, Merriam, Kansas) to restore and access the data.

Emergency Mode Operation

Lakemary maintains multiple locations. If the main campus location was unusable due to damage, long-term loss of power, etc., Lakemary contracts with its MSP, NetStandard, to implement Disaster Recovery in their cloud.

Testing and Revisions

Backup disk drives are monitored daily for usability. Operational and cost constraints make extra full testing of disaster recovery and emergency mode operation prohibitive, however, walkthrough and desktop exercises are conducted.

Applications and Data Criticality Analysis

Critical EPHI includes health data profiles, critical incident reports, service logs and billing information. This data is all located on the main Lakemary file server and is backed up at intervals each day.

EPHI Systems

Lakemary will verify that all EPHI systems are hosted and maintained through a contract with the EPHI provider and meet requirements above.

Device and Media Controls

Lakemary will regulate the movement of hardware and electronic media containing EPHI, considering the following areas: disposal, media re-use, accountability and data backup and storage. The purpose of these procedures is to prevent internal or external disclosures that violate the minimum necessary standard.

Disposal

When Lakemary disposes of workstations or hard drives, all drives containing EPHI will be erased using an erasing utility, or the drives will be removed and destroyed. All computers must be reviewed and erased, if necessary, by the IT team before they can be disposed.

Media Re-Use

Reusable storage devices must be erased by the IT team before they are returned to common storage areas.

Accountability

The Information Security Officer maintains a log of all technology equipment, including hardware and associated media. This log is used to track the movement of equipment. All movement of equipment is to be done by the Information Security Officer or under his/her supervision.

Data Backup and Storage

As part of the procedure to move technology equipment and associated media, the Information Security Officer ensures there is a backup of all systems to be moved. Backed up data is then reinstalled on appropriate equipment. Retired or replaced equipment is then cleaned and erased.

Evaluation

Lakemary's Information Security Officer, HIPAA Privacy Officer, and the Executive Team are responsible for periodically evaluating both the technical and non-technical security policies and procedures to determine that they meet the requirements of the security rule. These evaluations will be performed at least annually, and whenever significant new technologies are planned or implemented. Lakemary monitors for unwritten/informal practices. If such practices are deemed appropriate, they are then integrated into Lakemary's approved written practices.

Facility Access Controls

Lakemary will ensure that unauthorized physical access to EPHI and the facilities in which EPHI is housed is limited. Lakemary will ensure that properly authorized access to EPHI is allowed. Lakemary accomplished this through contingency operations, facility security plans, access control and validation procedures, and maintenance records.

Contingency Operations

In an emergency situation, the Facilities Director, COO, CEO, and Senior Director Information Systems may access the Lakemary administration building to retrieve servers and data. The COO or CEO and Senior Director Information Systems are authorized to place orders for replacement equipment or to contract with a computer service provider to access data.

Facility Security Plan

All Lakemary facilities are locked. The server room in the main administration building is kept locked with minimum access. All outside entrances to Lakemary are locked. Outside entrances and offices are locked at all other Lakemary locations. Main exterior doors are locked through Verkada and require a badge to enter the facility.

Access Control and Validation Procedures

Employees other than Directors, Maintenance and the Senior Director Information Systems are limited to physical access to their assigned work areas by use of locked offices. Based on Lakemary’s risk analysis, these controls are deemed adequate.

Maintenance Records

Lakemary does not maintain documentation of maintenance on security features. Based on Lakemary’s risk analysis, such records are not deemed reasonable and appropriate.

Information Access Management

Lakemary provides employees with appropriate access to EPHI in accordance with the “minimum necessary” requirements described in Privacy Practices. Lakemary’s procedures include access authorization and access establishment and modification.

Access Authorization

Access authorization is based on the minimum necessary EPHI required for an employee to complete their assigned duties utilizing Role-based Access Control (RBAC), and network objects (files) are configured to allow access to only specific roles. The Executive Team assign employees to security groups and determine the appropriate minimum necessary EPHI that each group must be able to access. Employees who telecommute or access Lakemary EPHI from remote locations are subject to these same procedures.

Access Establishment and Modification

The Senior Director Information Systems creates the groups on Lakemary servers and provides appropriate access for each group. The Senior Director Information Systems then enters the appropriate users in each group, thereby restricting each user to the appropriate EPHI. Any addition, deletions or changes to users or groups are communicated, from an authorized manager/director, to the Senior Director Information Systems through the Tech Support Ticket System.

Integrity

Lakemary creates electronic scans of PHI that has been received or generated in paper form. These paper copies are compared to EPHI to ensure that the electronic copies have not been altered. Upon verification, paper documents are securely shredded.

Person or Entity Authentication

All users of Lakemary's electronic data systems, including remote users, are authenticated by the use of unique usernames and 2FA using a combination of any of the following: Biometrics (Facial recognition or fingerprint), Pin code or passwords associated with usernames, plus a second authentication using a unique Authenticator App on their personal cell phone. Passwords must be at least 14 characters long and must include a combination of upper and lower case letters, numbers, and specialized characters.

Security Awareness and Training

Lakemary provides Quarterly Security Awareness Training using KnowBe4 SAT to employees. Security awareness and training encompass the following: security reminders, protection from malicious software, log-in monitoring and password management.

All Lakemary students, faculty, employees, contract employees, interns and volunteers are required to attend and complete all applicable in-service education, training, and/or licensing courses as defined and required by Lakemary, licensing and regulatory agencies, and state and federal law (e.g. compliance training and other training required based on job classification). Additionally, all contract employees must show evidence of general orientation and education, which may be accomplished by documentation of:

- Attendance at Lakemary educational offerings.
- Attendance at educational programs approved by Lakemarybut offered by the contractor; or
- Review of the Lakemary short-term contractor brochure with signature form.

Department Supervisors are accountable for providing the opportunity and direction to departmental staff to achieve the training and education required by these procedures. Service Directors must ensure that employees:

- Comply with institutional and departmental specific training and requirements; and
- Attend and complete the required training and have your attendance documented.

If the employee is unable to sufficiently complete the training requirement, it is the supervisor's responsibility to ensure that the employee receives the proper guidance needed to fulfill the requirement.

Lakemary provides a database for inputting and maintaining training information. Supervisors are accountable for reviewing the database to ensure that employees have participated in and completed all applicable training.

Security Reminders

Lakemary will provide periodic security reminders to employees who access EPHI. Reminders may be provided by email, interoffice memoranda, or through Lakemary training programs. Such reminders may include, but are not limited to, regularly changing passwords and password security issues, malicious software issues and proper logon and logoff procedures.

Protection from Malicious Software

Lakemary uses server-based and workstation-based applications to protect EPHI from malicious software. Such applications include, but are not limited to, regularly updated anti-virus software, email spam filter, and spyware detection software. Lakemary also employs an active firewall to reduce the risk of intrusion into its systems.

Login Monitoring

Lakemary’s server software provides login monitoring capability. The Senior Director Information Systems periodically reviews those logs to detect potential security incidents that involve unsuccessful login attempts.

Password Management

Lakemary workstations and servers require a login that includes an authentic username and proper corresponding password for access. In addition, access by remote locations is accomplished by a Virtual Private Network (VPN) which also requires login and authentication. Passwords are set by users and must meet specifications as required by Lakemary. Passwords must be changed every 365 days, at which time they expire. Users may not use a password if it was within the last 10 password changes.

Security Incident Procedures

The Senior Director Information Systems will work to mitigate (i.e., lessen or alleviate) any harmful effect that becomes known. This may include, but is not limited to, the following:

- Taking operational and procedural corrective measures to remediate the incident.
- Taking actions specified in the "Sanctions" procedure.
- Addressing problems with business associates.
- Incorporating the mitigation solutions into Lakemary's policies as appropriate.

Documentation of security incidents and their mitigation will be maintained by the Senior Director Information Systems.

Security Management

Risk Analysis

The purpose of Lakemary's risk analysis is to assess potential risks and vulnerabilities to the confidentiality, integrity and availability of EPHI. Lakemary has conducted a risk analysis of systems affecting EPHI as of the date of adoption of these procedures. As new systems for maintaining, transmitting or accessing EPHI are designed or implemented, Lakemary will conduct a risk assessment of those systems.

Risk Management

Lakemary will implement policies and procedures to reduce risks identified in its risk analyses to a reasonable and appropriate level.

Sanctions

Any persons included in the "Audience", as previously defined, be subject to sanctions in the event such persons fail to comply with these security policies and procedures. Lakemary's response to such failure to comply may include, but is not limited to, taking employment actions to re-train, reprimand or discipline persons as necessary, up to and including termination.

Information System Activity Review

The COO and the Senior Director Information Systems will regularly review records of information system activity. Records may include audit logs, access reports and security incident tracking reports. The purpose of this review is to monitor impending incidents or to detect and mitigate incidents that have occurred in a timely manner.

Transmission Security

Lakemary maintains measures to guard against unauthorized access to EPHI that is being transmitted electronically, based on its risk assessment. Paper copies of EPHI are used to verify the integrity of electronically transmitted EHPI. Any PHI transmitted via email outside Lakemary's servers must be encrypted.

Workforce Security

Lakemary maintains procedures to ensure that employees have appropriate access to EPHI. These procedures include authorization and supervision, workforce clearance procedures, and termination procedures.

Authorization and Supervision

These procedures specification applies to employees who do not normally have access to EPHI. This includes technology operations and maintenance personnel. Lakemary recognizes that technology operations personnel will need to have occasional access to EPHI files for routine and non-routine system maintenance. The Technology Administrator will be trained on EPHI security requirements and is authorized to access EPHI files for maintenance operations. The Senior Director Information Systems is responsible for adequately supervising any assistants or subcontractors who are used in maintenance operations.

Any other employees who do not normally have access to EPHI must obtain authorization from the Senior Director Information Systems prior to accessing EPHI. The Supervisor will determine the level of access necessary during such an employee’s period of access. A ticket must be submitted for this request through the Tech Support Ticket System then approved by the HIPAA Privacy Officer.

Workforce Clearance Procedures

Workforce clearance procedures begin with the screening and hiring process as outlined in the Lakemary Employee Handbook. Procedures also include reference checks and background checks as required by Lakemary’s licensing organizations.

At the time of hire, the employee’s supervisor will communicate to the Information Security Officer about the appropriate level of access to EPHI for that employee. A ticket must be submitted through the Tech Support Ticket System for this communication. Supervisors are also responsible for providing employees with appropriate physical access to Lakemary facilities through the use of keys.

Termination Procedures

Upon termination of employment, employees are to return all keys, files, physical access badges, and other Lakemary property to their supervisors. Supervisors are responsible for ensuring that all such items are returned. The supervisor will submit through the Tech Support Ticket System to notify the Senior Director Information Systems to disable the employee’s network user account and email account on Lakemary servers, and accounts on cloud- based EHR systems.

Workstation Security

Lakemary will ensure that all workstations that can access EPHI are located in a manner that protects them from physical access by unauthorized persons. Workstations are to be located in locked offices, unless they are prohibited from accessing EPHI. The prohibited areas include: front desk, copy room, tablets and dorms.

Workstation and Mobile Device Use

Lakemary workstations and mobile devices will be used in a manner that protects EPHI. Guidelines to accomplish this include, but are not limited to:

- All employees must log off their computers and mobile devices before leaving work. Employees shall also log off or lock their computer when leaving their work area or mobile device for any length of time, including lunch and breaks.
- Employees may not use their internet browser's "password store" functions to have passwords automatically remembered by their system. This includes employees accessing Lakemary's servers from remote locations or from home.
- Employees should orient screens and monitors in a way that prevents others from observing EPHI or install a privacy screen on their monitor.
- Passwords must be carefully guarded and protected. They shall not be shared with other employees. They shall not be written down and left in the area of the employee's workstation or mobile device.
- Employees must follow the acceptable use guidelines in the Lakemary Employee Handbook.

HIPAA Officers

HIPAA Privacy Officer – Sherri Johnson
Information Security Officer – Josh Patterson, Senior Director Information Systems
COO – Janet Broll