Data Security Policy - Access Control

PURPOSE
To provide principles and guidelines for access control activities at Organization**.**

SCOPE
The Access Control Policy will cover Organization's**:**

- User Identification and Unique IDs
- Access Management, including provisioning, modification, and termination
- Emergency Access
- Access Reviews
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY
Organization has adopted and follows processes for managing access to data and systems. Only authorized and appropriate workforce members have access to sensitive or protected information (including *ePHI*) and systems. The company aims to protect the confidentiality, integrity, and availability of sensitive and protected data, and has set up safeguards to restrict access to systems and assets.

Organization has set up role-based access control (RBAC) to limit access to only those workforce members who need it to complete their job function(s). Wherever possible, the company has employed the principle of "least privilege," reducing access to the minimum necessary.

Access to *ePHI* and other protected information is approved and granted only to those workforce members who require access to complete their job function(s) or role(s). Users who do not need access to *ePHI* are not given access.

Organization separates incompatible duties between one or more different workforce members.

User Identification and Unique IDs
Organization ties users' identities to their unique IDs at the company. Workforce members must use their unique IDs or user accounts to conduct their daily job functions. Unique IDs are used to

tie user activities and access logs back to individuals and are important for maintaining quality audit trails.

Access Management

Organization has set up processes to facilitate access requests, access grants or provisioning, access modification, and access termination. Access to sensitive or protected information and assets must be approved by an appropriate supervisor.

Organization has set up a mechanism for users to request additional access rights. These requests are formally documented through a ticketing system or similar repository.

Access Provisioning

Organization has set up a process to grant or provision access only when access is approved and appropriate. Users should only be given access to information or systems that they need to complete their job function(s).

Access provisioning activities are documented and captured through a ticketing system or similar repository.

Access Modification

Organization has set up a process to request and complete modifications to a user's access, either due to a role change, or other business reasons.

Access modification activities are documented and captured through a ticketing system or similar repository.

Access Termination

Organization has set up a process to remove, revoke, or terminate user access to information and systems upon the workforce member's termination, or other business reasons. Access termination is performed timely to prevent unauthorized access to sensitive and protected information.

Access termination activities are documented and captured through a ticketing system or similar repository.

Emergency Access

In the event that emergency access is required, and an appropriate approver is not immediately available, emergency access and subsequent activities performed with that access may be approved after the fact.

Cases of emergency access must be formally requested and documented through a ticketing system or similar repository.

Any emergency access activities will be reviewed by an appropriate workforce member.

Access Reviews

Organization performs periodic access reviews over users' access to information and systems. If any actions, such are modifying or terminating access, are necessary following the review, they

are carried out in a timely manner. User access reviewers must have the appropriate credentials and knowledge to complete the review.

Documentation of user access reviews and reviewer signoff is retained.

PROCEDURES

Organization has set up various processes for managing users' access, identifies, and authentication. Prior to receiving access to sensitive or protected information or systems, workforce members undergo a thorough screening process to verify their identities and skills.

Organization provides access to workforce members on the basis of their job function(s) or roles, and restricts access to sensitive or protected information through the access controls and processes described below.

User Identification and Unique IDs

Organization keeps an up-to-date, complete, and accurate listing of all users, accounts, and identities of workforce members at the company. As needed, each system owner should be able to generate a complete list of users with access to systems in their jurisdiction and their roles or access permissions. These listings will be used to manage and review user access across the organization.

The company uses a Single-Sign On solution that enables users to access multiple applications or systems using one set of secure credentials when feasible.

Password or Passkey Management

Whenever users are required to make a new password as part of their job duties or role, they must meet the following standards:

- Use a minimum of eight (8) characters, with longer passwords being more secure
- Disallow or do not use sequences or repetitive characters, such as "12345" or "aaaaa"
- Disallow or do not use context-specific passwords, like the name of the site or company
- Disallow or do not use commonly used passwords, such as "password123" and "12345678"
- Disallow or do not use single dictionary words
- Disallow or do not use passwords that have been compromised previously

The company provides workforce members with annual security training that provides instruction and guidelines for creating strong passwords.

Multi-Factor Authentication (MFA)

When possible, Organization enforces multi-factor authentication requirements for users and systems. Multi-factor authentication or MFA requires a user to have a second factor, like a phone

or security token, to log in to their account(s). Adding another factor to authentication and log in makes it more difficult for accounts to be compromised through password attacks alone.

Any systems that house sensitive or protected information, including *ePHI*, must have MFA enforced for all users. If MFA cannot be enforced due to technical limitations or other business reasons, these exceptions should be documented and added to the company's *Risk Register*.

Remote users must use MFA when accessing sensitive or protected information or assets.

Access Management

All systems that contain or process sensitive or protected information, including *ePHI*, must incorporate access controls that govern the provisioning, modification, and termination of user access.

Any systems that have built-in or default accounts must have those accounts either disabled or credentials and passwords changed to restrict and monitor access. Workforce members are discouraged from using group accounts or system accounts whenever possible and should only perform work activities through their own accounts. Workforce members are not permitted to share accounts or credentials.

All access control activities are captured and documented in Organization's ticketing system or similar repository.

When possible, Organization has automated access control workflows to route tasks and requests to appropriate workforce members, such as approvers and system owners.

Access Provisioning

All access to sensitive or protected information or systems must be formally requested, documented, and approved prior to granting access. These access granting or provisioning activities are captured in a new hire *Onboarding Checklist* or *Access Request*.

Access requests include:

- Name and user ID of the user creating the access request
- Name and user ID of the user who access is being requested for
- Description of the access request, including systems, roles, or permissions
- Justification for the access request

The system owner receives and reviews the access requests for their system(s). If the access request is appropriate, the request is routed to the authorized approver, and the request is approved.

Access is granted or provisioned as described in the approved access request.

If the access request is not approved, access will not be granted.

Access Modification

If a user's access needs to be modified or changed for any reason, such as a role change or a reorganization, an access request must be submitted to document the modification.

The system owner receives and reviews the access modification requests for their system(s). If the access request is appropriate, the access request is routed to the authorized approver, and the request is approved.

Access is modified as described in the approved access request.

If the access request is not approved, access will not be modified.

Access Termination

Organization has set up a process to automatically terminate user access throughout the organization once notification or termination or access removal has been received. All access held by the terminated user to the company's systems and assets is promptly terminated, removed, revoked, or disabled, no later than 24 hours from notification.

Termination requests and control activities are captured in the company's *Offboarding Checklist* and ticketing system or similar repository. Documentation should include the reason for the access change, such as a termination of employment or role change.

Emergency Access

Organization has set up a process to grant emergency access permissions to workforce members during an emergency situation or major incident. Emergency access requests must be formally documented and submitted through the ticketing system. Emergency access may be granted without approval if the justification and severity of the incident is sufficient.

All activities performed with emergency access are logged and monitored. Emergency access logs are reviewed no later than 10 business days after the incident, and any unauthorized activities or actions are investigated and remediated as needed.

Emergency access requests must be approved by an appropriate workforce member within 48 hours.

Emergency access is removed or revoked once the access is no longer needed, or the situation has been resolved, and is automatically revoked unless extended.

Access Reviews

Organization has set up a process for conducting company-wide user access reviews on an at least bi-annual basis. During this review, the company's overall identity directory should be reviewed for any terminated employees, and any job changes. These changes should be carried out as a result of the review.

In addition, each system containing or processing sensitive or protected information, including ePHI, must have access listings reviewed for any inappropriate access, unauthorized access, or terminated access. Any findings resulting from the system access review should be documented and carried out through the standard access control procedure. Any anomalous activity detected should be reported through the incident response and reporting process.

Only qualified workforce members, such as Human Resources and system owners, should perform user access reviews. Reviewers must sign off on the review and reflect the date the review as performed, as well as any changes that need to be completed as a result of the review. Reviewer signoffs are documented in our ticketing system.

ROLES AND RESPONSIBILITIES

User Access Reviewer: Determines if user access is appropriate during periodic access reviews. May be the application or system owner.

System Owner: Accountable for the system, including user access. May be the approver for access requests to their system(s).

FORMS/PLANS/DOCUMENTS

- Access Request
- Onboarding Checklist
- Offboarding Checklist
- User Access Reviews and Reviewer Signoff
- Emergency Access Log
- User Listings or Populations
- Risk Register

RELATED POLICIES AND PROCEDURES

- Data Security Policy – Security Management
- Data Security Policy – Information Access Management
- Data Security Policy – Facility Access Control
- Data Security Policy – Workforce Security
- Data Security Policy – Security Awareness and Training

- Data Security Policy – Contingency Plan
- Data Security Policy – ePHI Safeguards

RELEVANT HIPAA REGULATIONS

- 164.312(a)(1) *Access control*
- 164.308(a)(5)(ii)(D) *Password management*
- 164.312(d) *Standard: Person or Entity Authentication*
- 164.308(a)(3)(ii)(A) *Authorization and/or supervision*
- 164.308(a)(3)(ii)(B) *Workforce clearance procedure*
- 164.308(a)(3)(ii)(C) *Termination procedures*

RELEVANT SOC 2 CRTIERIA

- CC6.1.2 *Restricts logical access*
- CC6.1.3 *Identifies and authenticates users*
- CC6.1.5 *Manages points of access*
- CC6.1.6 *Restricts access to information assets*
- CC6.1.7 *Manages identification and authentication*
- CC6.1.8 *Manages credentials for infrastructure and software*
- CC6.2.1 *Controls access credentials to protected assets*
- CC6.2.2 *Removes access to protected assets when appropriate*
- CC6.2.3 *Reviews appropriateness of access credentials*
- CC6.3.1 *Creates or modifies access to protected information assets*
- CC6.3.2 *Removes access to protected information assets*
- CC6.3.3 *Uses role-based access controls*

APPENDIX A: CIRCUMSTANCES WARRANTING TERMINATION OF ACCESS TO EPHI

Workforce members' access to ePHI must be terminated:

1. If management has evidence or reason to believe that the user is using information systems or resources in a manner inconsistent with Organization's HIPAA Security Rule policies.

2. If the workforce member or management has evidence or reason to believe the user's password has been compromised.

3. If the user resigns, is terminated, is suspended, retires, or is away on unapproved leave.

4. If the user's job description changes and system Access is no longer justified by the new job description.

APPENDIX B: EXAMPLE TERMINATION ACTIVITIES

Specific termination procedures may include:

- Physical security measures, if any, including retrieving keys and pass cards, and changing locks

- Deactivation of computers and other electronic tools

- Deactivation of Access accounts

- Disabling of users and passwords

- Completion of an employee offboarding checklist. Organization will complete this checklist each time an employee leaves Organization. Checklist items should include at least the following:

    -

    - Return of all Access devices

    - Deactivation of logon accounts, including remote Access

    - Return of any computers and other similar electronic tools, such as a tablet or cell phone

    - Delivery of any data/information in the workforce member's possession or control.

Data Security Policy – Audit Control

PURPOSE
To provide principles and guidelines for creating, managing, reviewing, and retaining audit trails and audit logs.

SCOPE
The Audit Control Policy will cover Organization's:

- Audit log management
- Audit log review(s)
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY
Organization has set up auditing, logging, and monitoring mechanisms on assets that contain or process sensitive or protected information, such as ePHI. Audit logs provide date and time-stamped entries that capture details about the activities performed on that asset, and the users who accessed the asset.

Audit logs can be set up for many different types of assets, to monitor everything from system performance to user activity.

Audit Log Management
Organization decides which assets to collect audit logs from based on criticality to the company and whether the asset contains sensitive or protected information, such as ePHI. Any systems that contain sensitive or protected information or are critical to the operation of the company must have audit logging enabled.

Organization considers asset performance, user activity, and other factors when deciding what to log on which systems.

Audit logs are retained based on regulatory and operational requirements.

Access to audit logs is restricted to appropriate workforce members and audit logs cannot be altered without tracking and approval.

Audit Log Reviews

Organization has adopted and follows a process for reviewing audit logs for security incidents. If any incidents are detected or suspected as part of the review process, they are reported through the incident response and reporting process.

Audit logs may also be reviewed to investigate detected incidents and can provide valuable insight into the security of the company's information assets.

PROCEDURES

Organization has set up processes to log and review access and activities performed on information systems that contain sensitive or protected information, including ePHI. The company has set up audit logging over:

- The network, including any vulnerabilities and unauthorized access
- Systems or assets containing sensitive or protected information, including ePHI
- System performance
- Changes to sensitive or protected data, including ePHI
- Applications and software

Audit Log Management

Audit logs should be configured to include, at minimum:

- The data and time of access or activity
- The origin of access or activity
- The identity of the user performing the access to activity
- A description of the access or activity

Access to modify audit logs is restricted to appropriate workforce members only.

Audit logs are retained for compliance purposes, and to complete incident investigation and response. Logs should be retained for a minimum of six (6) years. Network device and systems logs can be retained for a minimum of one (1) year if retention costs are prohibitive.

Audit logs will be stored securely and encrypted where applicable.

Audit Log Reviews

Audit logs are reviewed at least quarterly for all systems that contain or process sensitive or protected information, including ePHI. Reviewers must be competent and capable of performing the review based on their job function(s) or role(s) and must document their reviews through the company's ticketing system or other similar tool. Reviews must be completed in a timely manner.

Any changes or further action resulting from audit log reviews should be recorded as part of the review and have a ticket submitted through the incident response and reporting process.

If criminal activity is detected as part of audit log reviews, appropriate action should be taken, including contacting law enforcement.

ROLES AND RESPONSIBILITIES

Audit Log Reviewer: Reviews audit logs and reports incidents. Generates audit logs for compliance and operational purposes as needed.

RELATED POLICIES & PROCEDURES

- *Data Security Policy – Incident Response and Reporting*

RELEVANT HIPAA REGULATIONS

- §164.312(b) *Audit controls*

RELEVANT SOC 2 CRITERIA

- CC7.1.2 *Monitors infrastructure and software*
- CC7.1.3 *Implements change-detection mechanism**s*
- CC7.1.4 *Detects unknown or unauthorized components*
- CC7.2.1 *Implements detection policies, procedures, and tools*
- CC7.2.2 *Designs detection measures*
- CC7.2.3 *Implements filters to analyze anomalies*
- CC7.2.4 *Monitors detection tools for effective operation*
- CC7.3.2 *Communicates and reviews detected security events*
- CC7.4.7 *Obtains understanding of nature of incident and determines containment strategy*

Data Security Policy – Business Associate and Third Party Risk Management

PURPOSE
To provide principles and guidelines for business associate and third party risk management, including vendors, service providers, and suppliers.

SCOPE
The Business Associate and Third Party Risk Management Policy and Procedure will cover Organization's:

- Definition of business associates and third parties
- Due diligence and third party/business associate selection
- Third Party Inventory
- Third Party Risk Management (TPRM)
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY
Organization has adopted and follows processes for managing relationships, agreements, and day-to-day operations with business associates and third parties.

Business Associates and Third Parties
Third parties are contractors, service providers, vendors, suppliers, and any other businesses or partners the company engages with.

Business associates are a subset of third parties that create, process, store, handle, or otherwise maintain PHI or ePHI. The HIPAA Security Rule provides specific guidance for what must be included in Business Associate Agreements or "BAAs," including measures for safeguarding PHI or ePHI (164.314(a)). Business Associates must comply with the requirements of the HIPAA Security Rule and properly safeguard PHI or ePHI handled on Organization's behalf.

Organization documents and retains written agreements with business associates and third parties.

Due Diligence and Third Party Selection
Organization has adopted and follows a third party or business associate due diligence and selection process that incorporates cross-functional stakeholders.

Organization performs due diligence throughout the third party or business associate selection process, using internal requirements, industry standards, and questionnaires to screen potential candidates.

Rationale for selecting a third party or business associate is documented and retained as part of the Third Party Inventory, Repository, or Database. Organization can use the Vendor module in The Guard for this purpose.

Third Party Inventory

Organization has set up a Third Party Inventory that contains details and information about each third party or business associate the company does business with. The Third Party Inventory includes a risk rating for each organization based on the criticality of their services or products to our own operations.

Third Party Risk Management

Organization has set up processes to manage the third party or business associate relationship lifecycle. The company designates an "owner" to manage the relationship with the third party and ensure compliance with our security requirements and obligations.

Third Party Onboarding

Organization has set up a process for onboarding new third parties or business associates with the company, which includes designating a third party relationship owner and adding the organization to the Third Party Inventory.

Third Party Monitoring and Review

Organization has set up processes for monitoring or auditing the products or services provided by third parties or business associates, as well as their compliance with our security agreements.

Third party relationships are periodically reviewed, and any changes resulting from that review are reflected in the Third Party Inventory.

Third Party Noncompliance or Incident Reporting

Organization has set up processes for responding to third party issues or noncompliance. Workforce members should report suspected incidents through the standard incident reporting process or contact the Security Official directly.

Third Party Offboarding

Organization has set up processes for terminating third party or business associate relationships. Termination processes include removing third party access and updating the Third Party Inventory.

PROCEDURES

This Business Associate and Third Party Risk Management Policy and Procedure must be reviewed and updated at least annually. The reviewer will record the date that the review was completed.

Third Party and Business Associate Agreements (BAAs)

Organization retains written third party and/or business associate agreements for each third party vendor, service provider, or partner.

Business associate agreements must include commitments from the BA to:

- Set up policies and processes to address the HIPAA Security Rule's requirements
- Provide HIPAA security training to all employees
- Perform a regular, documented HIPAA risk analysis to determine if PHI and *ePHI* are appropriately protected
- Report and disclose security incidents or events that could impact Organization within 30 days of notification or sooner if reflected in the BAA, or as required by the HIPAA Breach Notification Rule
- Uphold and adhere to the requirements of the HIPAA Security Rule and other security measures outlined in the agreement

When possible, seek inclusion of MFA enforcement.

Due Diligence and Vendor Selection

Cross-functional stakeholders work together to determine the criteria and standards that third parties and business associates must meet to be selected. Some criteria that should be considered as part of the vendor selection process are:

- Financial considerations, including cost, upkeep, and budget
- Compliance risks, including adherence to the HIPAA Security Rule and third party or business associate agreements
- Industry standards and best practices
- Resources and capabilities available to the company
- Alternative solutions, products, or services

As part of due diligence, Organization obtains any attestations or certifications held by the third party, such as SOC 1 or SOC 2 Type II reports, ISO certifications, HITRUST certification, or others. We review these reports or certifications and incorporate any findings into the overall vendor selection process. Reviewers of third party reports and certifications must record their findings and justification for their recommendations and retain this documentation as part of the Third Party Inventory. It can be uploaded to the vendor record in the Vendor module of the Guard.

Due Diligence Questionnaires In the event that a third party does not have a relevant third-party attestation, report, assessment, or certification to indicate their compliance with an industry

standard, the company may issue a custom “Due Diligence Questionnaire” that covers topics of interest to Organization. The Guard has a questionnaire available.

Third Party Inventory

Organization maintains a Third Party Inventory, Repository, or Database that lists all third party organizations, business associates, partners, vendors, suppliers, and contractors that the company does business with. Organization tracks this information in the Guard Vendor module or alternate tracking tool. The Third Party Inventory should contain or link to the following details and information about each organization:

- Third party name and description
- Third party relationship owner
- Third party contact information
- Signed contract or agreement
- Risk rating, based on the criticality of the third party’s products or services to **Organization’s** operations
- Review notes
- Due diligence documentation

The company may opt to track other parameters as well.

Third Party Risk Management

Organization’s Third Party Risk Management process and lifecycle includes third party onboarding, monitoring and review, and offboarding. These steps may occur simultaneously for different third parties.

Third Party Onboarding

When a new third party or business associate enters into an agreement with Organization, they are added to the Third Party Inventory.

If any access is required for third party users or services, the relationship owner will submit requests and follow the company’s Data Security Policy - Access Control on behalf of the third party.

The relationship owner facilitates access requests to the third party’s resources, applications, or services as needed.

Third Party Monitoring and Review

The company regularly monitors the performance of third parties, as well as their compliance with the written agreement.

At least annually, third party contracts, agreements, and relationships are reviewed, and any observations or changes resulting from that review are reflected in the Third Party Inventory.

Third Party Noncompliance or Incident Reporting

If a third party is found to be in noncompliance, Organization will first attempt to address the issue. Business associates that fail to comply with HIPAA requirements may be terminated, or have findings reported to the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) within 30 days of the incident.

If an Organization workforce member receives a report or complaint of third party or business associate noncompliance, that event should be reported promptly through defined incident reporting channels, or directly to the Security Official. The Security Official is responsible for responding to the situation and initiating Incident Response and Reporting procedures.

The third party relationship owner will work with the third party for support, troubleshooting, and customer service as needed.

Third Party Offboarding

When a third party or business associate needs to be offboarded or terminated for any reason, all access to Organization's information and assets must be removed upon notification. Changes to that third party's status are updated and reflected in the Third Party Inventory.

The third party relationship owner should work with cross-functional stakeholders, such as Accounting and Legal, to coordinate the termination of third party payments and ensure that all legal considerations are addressed.

ROLES AND RESPONSIBILITIES

Security Official: Receives complaints or reports related to third party or business associate noncompliance or failure to safeguard ePHI. Responds to third party security incidents or delegates responsibilities.

Third Party Relationship Owner: Maintains the company's relationship with designated third party organizations. Ensures third party compliance with contractual agreements and HIPAA Security Rule requirements. Monitors third party performance and reports incidents as needed.

VIOLATIONS

Business associates that fail to comply with HIPAA requirements may be terminated, or have findings reported to the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) within 30 days of the incident.

FORMS/PLANS/DOCUMENTS

- Third Party Inventory. The Guard's Vendor Module can be used create this.
- Business Associate Agreement or Third Party Agreement Templates are available in the Guard document module.

RELATED POLICY

- *Data Security Policy - Security Management*

RELEVANT HIPAA REGULATIONS

- § 164.308(b)(1) *Business associate contracts and other arrangements*
- § 164.308(b)(3) *Written contract or other arrangement*

RELEVANT SOC 2 CRITERIA

- CC9.2.1 *Establishes requirements for vendor and business partner engagements*
- CC9.2.2 *Assesses vendor and business partner risks*
- CC9.2.3 *Assigns responsibility and accountability for managing vendors and business partners*
- CC9.2.4 *Establishes communication protocols for vendors and business partners*
- CC9.2.5 *Establishes exception handling procedures from vendors and business partners*
- CC9.2.6 *Assesses vendor and business partner performance*
- CC9.2.7 *Implements procedures for addressing issues identified during vendor and business partner assessments*
- CC9.2.8 *Implements procedures for terminating vendor and business partner relationships*
- CC9.2.9 *Obtains confidentiality commitments from vendors and business partners*
- CC9.2.10 *Assesses compliance with confidentiality commitments of vendors and business partners*
- CC9.2.11 *Obtains privacy commitments from vendors and business partners*
- CC9.2.12 *Assesses compliance with privacy commitments of vendors and business partners*

Data Security Policy - Contingency Plan

PURPOSE
To provide principles and guidelines for how emergency response procedures and contingency plans will be created, adopted, followed, and maintained.

SCOPE
The Contingency Plan Policy will cover Organization's**:**

- Data backup plan
- Disaster recovery plan
- Emergency Mode Operation plan
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- And Relevant Regulations, Standards, and Criteria

POLICY
Contingency plans, policies, and procedures are designed to guide Organization through emergencies and disasters that could affect the business.

During emergencies or disasters, systems and physical assets containing PHI and ePHI may be damaged or disrupted in some way. Organization's contingency plans will make sure that we are prepared for an emergency.

Your contingency plan must include all of the following components.

Data Backup Plan
Organization will create a data backup plan or procedure, which describes the process for backing up information systems and data. Backup frequency for each system is determined by the criticality of the system and impact of data loss, as defined in each system's risk analysis.

Disaster Recovery Plan
Organization will adopt and follow a Disaster Recovery Plan, which describes how the business will recover from an emergency or disaster event. This written plan makes sure that Organization can recover from the loss of data or disruption due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster affecting systems containing sensitive or protected information, including ePHI.

Emergency Mode Operating Plan

Organization will adopt and follow a written Emergency Mode Operating Plan, also known as a Business Continuity Plan, which directs how Organization and its employees should operate in an emergency scenario. The plan will cover how PHI and ePHI will be secured and handled while Organization remains in emergency mode.

PROCEDURES

Organization's Contingency Plan Policy will be reviewed and updated at least annually, or when significant changes occur.

Data Backup Plan

Organization uses a backup tool to manage digital backups where feasible.

Organization will create and maintain retrievable exact copies of ePHI and other data necessary for operations. Backups are sufficient to restore information systems to a recent and operational state. Organization will hold these backups offsite in a secure location, or with a HIPAA-compliant cloud vendor.

Organization will implement backups and replication for all cloud storage (Google, Microsoft 365, Dropbox, etc.) and cloud services (AWS, GCP, Azure, etc.) used.

Organization performs backups of systems and data containing sensitive and protected information at least daily, or continuously when possible.

Organization secures any backup media in a safe location separate from the system that created the backup. We track backup locations, activity, and files. You may use The Guard's asset module to assist with this control activity.

All backups are secured and encrypted, with any exceptions documented.

Disaster Recovery Plan

Organization will develop, adopt, and follow the disaster recovery plan consisting of the following components:

- **A communication plan** that includes:
    -
    - Who should be notified of a disaster
    - Employee contact information
- **Data backups** and where they are stored
- **Role descriptions** that cover:
    -

    - Who is responsible for assessing damage
    - Who is responsible for system recovery
    - Who is responsible for other key roles in the recovery process
- **A detailed asset inventory,** or a way to access it, that includes details about:
    -
    - Computers
    - Workstations
    - Devices
    - Hardware
    - Printers
    - Scanners
    - Other **Organization** assets
- **An equipment plan** for protecting:
    -
    - Desktop and laptop computers
    - Devices
    - Printers
    - Other equipment that can be damaged in a disaster
- **A data restoration priority plan** that lists systems in the order they should be restored in, if feasible
- **A vendor communication plan** that includes:
    -
    - A list of vendors that need to be contacted
    - Vendor contact information

    - Vendor communication prioritization (e.g., who should be contacted first)

- **A plan for document storage, access, training, and review** that includes:

    -

    - Where the plan will be stored on-site

    - Where the plan will be stored off-site

    - Where employees can find the plan

    - How employees are trained on the plan and how often

    - When the plan is reviewed and updated

Emergency Mode Operating Plan (Business Continuity Plan)
Organization will adopt and follow a written business continuity plan, also known as an Emergency Mode Operating Plan that includes:

- **Definitions of critical business processes** that need to operate during an emergency for the security of ePHI and other sensitive information

- **Designating who should be responsible** for recovering and/or continuing critical business process operations

- **Steps for recovering and operating** critical business processes

- **Testing the plan** for continued effectiveness and opportunities for improvement

We will test the Emergency Mode Operating Plan at least annually. Changes to the plan require approval from the Security Officer.

Periodic Testing and Revision of Contingency Plan
The data backup plan, disaster recovery plan, and business continuity plans will undergo periodic testing and revision.

- Each plan will be tested no less than annually.

- Each plan will be tested whenever changes are made to the plan. Testing will include workforce members, to ensure they understand their roles and responsibilities. If testing reveals that the Contingency Plan will be ineffective in the event of an emergency or other occurrence, the Security Official will revise the plan accordingly.

- Backup plan testing will include backup media testing. **Organization** will ensure that backup media will be tested periodically for accessibility and integrity. If there are readability issues,

backup media will be replaced to ensure sufficient backup data is available to enable the restoration of the system to a recent, operable, and accurate state. Backup recovery testing will occur at least quarterly.

ROLES AND RESPONSIBILITIES

Security Official: Responsible for establishing, reviewing, and approving changes to the Contingency Plan Policy.

FORMS/PLANS/DOCUMENTS

Contingency Plan Annual Test

System-Specific Disaster Recovery Plan

Emergency Mode Operating Plan

RELATED POLICY

Data Security Policy - Security Management

Data Security Policy - Access Control

Data Security Policy - Device and Media Control

RELEVANT HIPAA REGULATIONS:

- §164.308(a)(7)(i) *Contingency plan*
- §164.308(a)(7)(ii)(A) *Data backup plan*
- §164.308(a)(7)(ii)(B) *Disaster recovery plan*
- §164.308(a)(7)(ii)(C) *Emergency mode operation plan*
- §164.308(a)(7)(ii)(D) *Testing and revision procedures*
- §164.308(a)(7)(ii)(E) *Applications and data criticality analysis*
- §164.310(a)(2)(i) *Contingency operations*

RELEVANT SOC 2 CRITERIA

- CC 7.3.1 *Responds to Security Incidents*
- CC 7.4.5 *Restores Operations*
- CC 7.5.1 *Restores the Affected Environment*

- CC 7.5.2 *Communicates Information About the Event*
- CC 7.5.3 *Determines Root Cause of the Event*
- CC 7.5.4 *Implements Changes to Prevent and Detect Recurrences*
- CC 7.5.5 Improves Response and Recovery Procedures
- CC 7.5.6 Implements Incident Recovery Plan Testing

Data Security Policy - Device and Media Control

PURPOSE

To provide principles and guidelines for device and media controls and safeguards at Organization, including endpoint and mobile devices.

SCOPE

- The Device and Media Control Policy will cover Organization's**:**
- Device, hardware, and media controls and handling
- Device, hardware, and media tracking and documentation
- Device, hardware, and media usage and disposal
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY

Organization has and follows a process for managing physical devices, hardware, and media that contain sensitive or protected data, such as ePHI*.* The company tracks and documents all devices, hardware, or media in use at Organization, and stores this information in our *Asset Management Repository*. We may choose to use the Guard's Asset module for this purpose.

When necessary, additional training is provided to personnel and users that are responsible for managing and disposing of devices, hardware, and/or media.

Any instances of loss or theft of devices must be reported immediately.

Device, Hardware, and Media Management
Organization has and follows a process for onboarding new devices, hardware, or media into the environment. Devices must be configured and hardened to the level defined by the company before being used in a production environment. Devices are stored in secure physical locations. Devices, hardware, and media are tracked in the company's *Asset Management Repository*. We may choose to use the Guard's Asset module for this purpose.

Any devices that are re-used are sanitized of sensitive or protected data prior to re-use.

Device, Hardware, and Media Disposal
Organization has and follows processes for disposing of devices, hardware, and media, including those that house sensitive or protected information, such as ePHI*.* Disposal processes include the sanitization and removal of sensitive or protected data. Disposal of physical assets are conducted securely and tracked.

Devices, hardware, or media that contained ePHI must have ePHI rendered unusable, unreadable, or inaccessible for proper disposal.

Device, Hardware, and Media Tracking and Documentation
Organization has and follows processes for documenting devices, hardware, and media control activities. Documentation includes a chain of custody, which indicates the individual responsible for the device and the location of the device.

Organization retains any documentation related to the management of devices, hardware, and media, from procurement to disposal or decommissioning.

Device, Hardware, and Media Backups
Organization has adopted and follows a process for backing up sensitive or protected information, such as ePHI*,* in compliance with the HIPAA Security Rule.

PROCEDURES

Organization has set up a process to track all devices, hardware, media, and assets at the company in our *Asset Management Inventory* or Repository. The Guard has an Asset Module available for this use.

Any instances of loss or theft of devices must be reported immediately through the incident management reporting workflow.

Device, Hardware, and Media Management
When new devices, hardware, or media are added to the Organization's environment, they are also added to the company's *Asset Management Inventory*. The *Asset Management Inventory* should include the following details for each asset:

- Unique ID
- Serial number
- Operating system
- Database type
- IP address
- Production / Development / Test / QA
- Contains / Does not contain ePHI
- Asset name
- Department or business unit
- Owner
- Other important details

Devices are hardened to the configuration and integrity standards defined by the company for each asset type. Hardening involves configuring assets to a secure baseline. Hardening occurs before the asset is used in production environments. Device hardening and configurations are tracked or linked through the *Asset Management Inventory*.

Any physical assets are stored in secure, locked locations. These storage locations should only be accessed by workforce members authorized to handle physical devices, hardware, or media.

Device, Hardware, and Media Disposal

Organization has set up processes for disposing of devices, hardware, and media, including those that house sensitive or protected information, such as *ePHI.* The disposal process includes the sanitization, purging, or destruction of sensitive or protected information from the device, hardware, or media. Disposal processes are tracked in the *Asset Management Inventory* and ticketing system (or similar tool) as they occur.

Once devices, assets, or media are sanitized, the physical asset may need to be disposed of. Organization will use a secure disposal or destruction service to destroy any devices, hardware, or media that need to be physically destroyed, and retain certificates of destruction for physical assets destroyed.

Device, Hardware, and Media Tracking and Documentation

Organization has set up processes for tracking devices, hardware, and media, and documenting control activities. The *Asset Management Inventory* contains all key information about devices, hardware, and media in use at the company. A ticketing system or similar tool is in place for tracking the movement or disposal of devices, hardware, and media.

Documentation includes a chain of custody, which indicates the individual responsible for the device and the location of the device.

Devices, hardware, or media that contain or process sensitive or protected information must have a request and approval documented and tracked if the physical asset is moved from one facility to another.

Device, Hardware, and Media Backups

Organization has set up a process for creating exact copies or backups of sensitive or protected information, including ePHI. Backups are stored securely and encrypted to safeguard sensitive or protected data. Additional backup and recovery procedures can be found in The Guard under the Data Security Policy - Contingency Plan.

Definitions

Clearing

Clearing sanitizes data, protecting against simple, non-invasive data recovery techniques. Clearing is typically applied through standard Read/Write commands to the storage device. This may include rewriting with a new value or using a menu option to reset a device to the factory state (when rewriting is not supported). The data is then overwritten and verified. Most devices support some level of clearing sanitization. Clearing sanitization has a limit, however – it does not reach hidden areas or areas that cannot be addressed.

Purging

Purging applies techniques that render data recovery infeasible. Purging provides a more thorough level of sanitization than clearing and is used for more confidential data. Purging requires the removal of hidden drives, if these are present. Purging may not work on all firmware.

Destroying

Destroying renders target data recovery infeasible. Destroying also renders the media incapable of storing data afterward. “Destroying” includes a variety of techniques, such as shredding, incinerating, pulverizing, melting, and other physical techniques. These techniques may be necessary for drives that are already beyond all possible use or standard overwriting methods because of physical damage.

ROLES AND RESPONSIBILITIES

Device Owner: Responsible for handling assigned devices, hardware, or media. Ensures compliance with Organization’s policies and procedures.

FORMS/PLANS/DOCUMENTS

- Asset Management Repository or Inventory (The Guard’s Asset module can be used for this purpose.)

RELATED POLICIES OR PROCEDURES

- Data Security Policy - Contingency Plan

RELEVANT HIPAA REGULATIONS

- § 164.310(d)(1) *Device and media controls*
- § 164.310(d)(2)(i) *Disposal*
- § 164.310(d)(2)(ii) *Media reuse*
- § 164.310(d)(2)(iii) *Accountability*
- § 164.310(d)(2)(iv) *Data backup and storage*

RELEVANT SOC 2 CRITERIA

- CC2.1.1 *Identifies information requirements*
- CC2.1.4 *Maintains quality throughout processing*
- CC3.2.6 *Identifies and assesses criticality of information assets and identifies threats and vulnerabilities*
- CC6.1.1 *Identifies and manages the inventory of information assets*
- CC6.5.1 *Identifies data and software for disposal*
- CC6.5.2 *Removes data and software from entity control*
- CC6.7.3 *Protects removal media*
- CC6.7.4 *Protects mobile devices*

Data Security Policy – ePHI Safeguards

PURPOSE
To provide principles and guidelines for protecting and safeguarding ePHI and other sensitive or protected information.

SCOPE
The ePHI Safeguards Policy will cover Organization's:

- Obligations for safeguarding ePHI and other sensitive or protected information
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY/PROCEDURES
Organization has adopted and follows processes for protecting *ePHI* and other sensitive or protected information from tampering or unauthorized access. The company safeguards the confidentiality, integrity, and availability (CIA triad) of ePHI that Organization creates, processes, receives, or transmits.

Organization only permits authorized access to *ePHI* and systems that contain *ePHI*.

Organization has set up processes and security mechanisms to ensure that *ePHI* is properly transmitted and encrypted.

VIOLATIONS
Noncompliance with the HIPAA Security Rule or violation of ePHI safeguards may result in disciplinary action or sanction.

RELATED POLICY

- Data Security – Device and Media Control Policy

RELEVANT HIPAA REGULATIONS:

- 45 CFR 164.312(a)(2)(iv) *Encryption and Decryption*
- 45 CFR 164.312(e)(2)(ii) *Encryption*

- 45 CFR 164.310(d) *Device and Media Controls*

Data Security Policy – Facility Access Controls

PURPOSE

To provide principles and guidelines for managing access to Organization's facilities, including those that house information systems. To provide detailed instructions for managing access to Organization's facilities, including those that house information systems containing ePHI or sensitive information.

SCOPE

The Facility Access Controls Policy and Procedures covers Organization's:

- Facility access controls, including *visitor access*
- Facility security plans
- Contingency operations
- Maintenance records
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY

Organization is dedicated to maintaining the *confidentiality, integrity, and availability of ePHI*. Organization adopts and follows a process for controlling access to facilities and physical locations that hold information systems. These controls are enforced through technical and physical methods. Only *authorized and appropriate* personnel are given access to Organization's facilities and physical sites.

Facility Access Controls

To control access to facilities and physical equipment, including information systems*,* Organization has procedures for provisioning access, modifying access, terminating access, and reviewing access, including visitor access.

Only appropriate personnel are given access to facilities or parts of facilities containing information systems that host sensitive information or ePHI. Facility access must be approved by someone who is authorized to do so.

Provisioning Facility Access
Organization has adopted a process for approving and granting access to facilities based on an individual's role or function.

Access provisioning is formally documented and retained.

Modifying Facility Access
Organization has adopted a process for changing access to facilities as needed, including requesting the change, approving the change and executing the change. Access modifications may be requested when someone in the company changes roles, needs access to another physical site, needs temporary access to a facility, and other circumstances with a valid business justification.

Access modification is formally documented and retained.

Terminating Facility Access
Organization has adopted a process for removing or disabling access to facilities as needed. Access to facilities is removed within 24 hours of receiving the notification.

Access termination is formally documented and retained.

Reviewing Facility Access
Organization has adopted a process for reviewing and validating access to facilities on a periodic basis. Facility access should be limited to individuals who need access to perform their job or role. As part of this facility access review, any changes to access that are needed should be made.

Facility access reviews are formally documented and retained.

Visitor Access
Organization has adopted a process for controlling and monitoring visitor access to facilities and physical sites containing sensitive information or ePHI.

Visitor access logs are formally documented and retained.

Facility Security Plans
Organization has put in place facility security plans and safeguards that protect the facility and equipment and physical assets held at the site from unauthorized physical access, tampering, and theft. Any information systems or electronic media that contain ePHI or sensitive information are stored in secure physical locations.

Facility Contingency Operations
Organization has adopted and follows a Data Security Policy – Contingency Plan that provides guidance for how to respond in the event of an emergency or disaster. As part of disaster

response and recovery, Organization has set up a contingency operations plan to recover any loss of data resulting from an emergency.

Organization has put in place a process to access facilities and physical sites holding ePHI or sensitive information during an emergency in support of the Business Continuity Plan (Emergency Mode Operating Plan), including requesting, approving, granting, monitoring, and terminating emergency facility access. Only authorized personnel will be given emergency facility access.

Facility Maintenance

Organization tracks and manages any security-related repairs, modifications or maintenance performed at facilities or physical sites that contain ePHI or sensitive information.

Facility maintenance records will be formally documented and retained.

PROCEDURES

Organization maintains the following facility access control procedures for its facilities and physical sites that contain information systems that store or process ePHI and other sensitive information.

Facility Access Controls

Organization keeps all documentation related to facility access in its ticketing system or a related tool.

Requesting Facility Access

To request access or modification of access to a facility or physical site, an individual or their manager must submit a formal request through the ticketing system or other tool. This request should include:

- Name or ID of the user receiving access
- Facility, site or area the user will access
- Requestor ID
- Date of request
- Business justification for access request

These requests are routed to the appropriate approver.

Provisioning or Modifying Facility Access

Upon receiving a request to provision or modify facility access, the Facility Manager or their delegate(s) review the request details and determine if the request should be approved or denied. Only appropriate personnel are approved for access to facilities that store ePHI or other sensitive information.

If the request is approved, the user will have their access granted or modified according to the request details. Any further changes to access will need a new request form.

If the request is denied, the user will not receive access.

Terminating Facility Access

In the event that an individual's access to a facility or physical site must be removed, terminated or disabled, their access will be revoked upon notification.

Reviewing Facility Access

On a **quarterly** basis, Organization reviews the list of people with access to facilities that contain ePHI or other sensitive information and makes sure that the list is complete and up to date. As part of the facility access review, the assessor will ensure that people who have access are:

- Not terminated employees or contractors
- Appropriate to have access based on their role or job function
- Appropriate to have access due to another business reason

If any changes need to be made coming out of the access review, those changes are made in a timely manner and documented.

As part of the facility access review, physical keys are inventoried to ensure that they are being held securely and by the appropriate individuals.

The facility access reviewer documents their review and signs off on the results.

Visitor Access

Before visitors can access Organization's facilities or sites with ePHI or other sensitive information, they must present photo ID, sign in to the visitor's log, and include the following details:

- First name
- Last name
- Date and time of arrival
- Data and time of departure
- Reason for visiting
- Main contact
- Signature or Initials

Visitors are to be escorted through any common areas or any areas that contain ePHI or other sensitive information or systems.

Facility Security Plans

Organization secures its facilities and physical sites containing information systems hosting ePHI or other sensitive information using a combination of controls and mechanisms.

Facilities and offices are locked to entry unless you have a badge or key. When appropriate, authorized employees and contractors receive unique badges to enter sites. Employees should not share access badges or allow "piggy backing" when entering a facility.

Alarms and surveillance cameras (where appropriate) ensure that the premises are protected.

If a physical key is lost or stolen, we will change the affected locks.

If an individual loses their badge or access card, we will disable the old card immediately and issue a new badge.

Data Centers, Network Cabinets, and Server Rooms

Data centers, network cabinets, and server rooms are kept locked. Access is only provisioned to a limited number of privileged users. All access to these areas is logged.

Facility Contingency Operations

Organization keeps and updates a Data Security Policy – Contingency Plan that provides instructions for operating in the event of an emergency.

During an emergency, appropriate people will be given access to facilities in order to support the objectives of the Business Continuity (Emergency Mode Operation) Plan. These authorized individuals will work to restore any loss of data, protect the confidentiality, integrity, and availability of ePHI, and fulfill their obligations listed in the Business Continuity Plan. When possible, we will log the activities and actions taken during emergency facility access.

Facility Maintenance

In the event that facility maintenance, repairs, or modifications are required at sites that contain information systems housing ePHI or other sensitive information, the details of those maintenance activities will be documented and tracked by the Facility Manager. This log should include:

- Name(s) of the maintenance personnel on-site
- Maintenance company
- Date and time of arrival
- Date and time of departure
- Description of repairs

- Reason for repairs
- Outcome of repairs and maintenance

ROLES AND RESPONSIBILITIES

Facility or Site Manager: Reviews and approves facility access, provisioning requests, modification requests, and terminations. Accountable for tracking and managing facility maintenance.

VIOLATIONS

Access to facilities and physical sites that contain ePHI or other sensitive information is limited to authorized personnel only.

Organization may take disciplinary action if personnel access facilities, physical sites, devices or equipment when they are not authorized to do so.

FORMS/PLANS/DOCUMENTS

- Facility Security Plan(s)
- Facility Visitor Access Logs
- Facility Access Logs and Documentation
- Business Continuity Plan (Emergency Mode Operating Plan)
- Maintenance Records and Logs

RELATED POLICY

- Data Security Policy – Contingency Plan

RELEVANT HIPAA REGULATIONS

- §164.310(a)(1) *Facility access controls*
- §164.310(a)(2)(ii) *Facility security plan*
- §164.310(a)(2)(iii) *Access control and validation procedures*
- §164.310(a)(2)(iv) *Maintenance records*

RELEVANT SOC 2 CRITERIA

- CC 6.4.1 *Creates or Modifies Physical Access*

- CC 6.4.2 *Removes Physical Access*
- CC 6.4.3 *Reviews Physical Access*

Data Security Policy – HIPAA Security Rule Basics

PURPOSE
To provide an overview of the HIPAA Security Rule and its requirements.

SCOPE
The HIPAA Security Rule Basics Policy covers Organization's

- Basic obligations under the HIPAA Security Rule
- Designated Security Official
- Required versus Addressable standard components
- Roles and Responsibilities
- Relevant Regulations, Standards, and Criteria

POLICY
The HIPAA Security Rule requires in-scope organizations such as Covered Entities and certain Business Associates to protect the CIA triad of confidentiality, integrity, and availability of electronic protected health information (ePHI). These combined technical, administrative, and physical measures are designed to safeguard PHI and ePHI.

Organization has set up policies and procedures to carry out the requirements of the HIPAA Security Rule, including responding to and reporting security incidents. These policies and procedures are retained in written form and reviewed and updated periodically.

Basic Requirements of the Security Rule
Under the HIPAA Security Rule, the Organization must:

- Ensure the confidentiality, integrity, and availability of ePHI that the company creates, processes, receives, or transmits
- Prevent and address any threats to the security or integrity of ePHI
- Prevent against unauthorized disclosure of ePHI

- Enforce compliance with the HIPAA Security Rule across the company's workforce

Designated Security Official
Organization has appointed a designated Security Official to develop and enforce the company's data security policies and procedures. The Security Official should be sufficiently senior in the company. The designated Security Official is listed below:

Name:

Title:

Email or Phone:

Required vs Addressable Standards
The HIPAA Security Rule standards include required and addressable components.

Organization sets up appropriate controls for required components, taking into account the company's current resources and capabilities, as well as potential risks to *ePHI.*

Organization assesses addressable components for feasibility. If the component can be addressed by Organization, the company will set up appropriate controls. If the component cannot be feasibly addressed, the reasons will be documented and retained.

Definitions
Administrative Safeguards - The HIPAA Security Rule *administrative safeguards* consist of administrative actions, policies, and procedures. These actions, policies, and procedures are used to manage the selection, development, and implementation of security measures.

The *administrative safeguards* regulation can be found at 45 C.F.R 164.308. This provision is subdivided into 45 CFR 164.308(a) and 45 CFR 164.308(b).

Physical Safeguard - Physical safeguards protect the physical security of offices and other locations where *ePHI* may be stored or maintained. Common examples of *physical safeguards* include:

- Alarm systems
- Surveillance cameras
- Access control systems
- Security systems
- Locking of areas where *ePHI* is stored

Technical Safeguards- Technical safeguards include measures, such as endpoint protection, firewalls, encryption, and data backup, that ensure that ePHI is properly accessed, monitored, and maintained.

ROLES AND RESPONSIBILITIES

Security Official: Sets up and enforces security policies and procedures in accordance with the HIPAA Security Rule. Reviews relevant policies and updates documentation as needed. Oversees incident response and reporting mechanisms. Main point of contact for security-related communications.

VIOLATIONS

Failure to comply with the HIPAA Security Rule or Organization's policies and procedures may result in disciplinary action or sanctions.

RELEVANT HIPAA REGULATIONS

- 45 CFR §164.308 *Administrative safeguards*
- 45 CFR §164.308(a)(2) *Assigned security responsibility*
- 45 CFR §164.310 *Physical safeguards*
- 45 CFR §164.312 *Technical safeguards*

Data Security Policy - Incident Response and Reporting

PURPOSE

To provide principles and guidelines for incident response and reporting at Organization, including security incidents. To provide detailed instructions for conducting incident response and reporting activities.

SCOPE

This Incident Response and Reporting Policy will cover:

- Detection, identification, response, and reporting of incidents and potential incidents **(Incident Management)**
- Mitigation of incidents that occur (**Incident Response)**
- Documentation of incidents

- Incident Management Process
- Incident Documentation
- Incident Response Process
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- And Relevant Regulations, Standards and Criteria

POLICY

Organization defines a “security incident” or “incident” as any event that results in unauthorized access, usage, disclosure, alteration, or destruction of information; or any disruption of information systems, including physical tampering.

Organization encourages a security-aware culture, so if you suspect an incident has occurred, contact your supervisor, or use the reporting hotline. Organization has included incident response in security training.

If Organization decides to follow industry data security best practices beyond the Security Rule, like SOC2, it will also perform periodic tabletop (TTX) exercises to simulate incident response activities.

Organization makes this Incident Response Policy and Procedures available to employees.

Incident Management

Organization adopts and follows an incident management procedure that provides instruction on:

- Detecting a security incident
- Identifying a security incident
- Documenting a security incident
- Responding to a security incident
- And reporting a security incident

Security incidents that involve ePHI may need to be handled in a specific way. Refer to the Data Security Policy – HIPAA Incident Response, Reporting, and Breach Determination Policy.

Examples of Security Incidents:

- Unauthorized access to physical or electronic assets, data, information, facilities, or accounts
- Cyber attacks, such as DDoS attacks, malware, social engineering, and others.
- Loss or theft of Organization devices or media
- Outages or disruptions of information systems and technology

Incident Response

Organization maintains a formal "Incident Response Plan" that are documented below *Procedure* section. Confirmed incidents are documented, and appropriate personnel are contacted to handle the incident. The incident team convened to address an incident is known as the "Incident Response Team" or IRT. IRTs can consist of members from all departments, levels, and regions across the organization.

Organization incident response consists of:

- Convening the IRT, including contact information plans
- Investigating the incident, including root cause
- Containing the incident
- Eradicating the incident
- Recovering from the incident
- And applying lessons learned from the incident

Incident Documentation

Organization documents each incident through to completion. Documentation of an incident should include sufficient information to determine the following:

- When the incident occurred and for how long
- What caused the incident
- What **Organization** did to respond to the incident
- How the incident was resolved
- And lessons learned from the incident

PROCEDURES

Organization makes these Incident Response and Reporting Procedures available to employees and includes them as part of *Security Awareness and Training.*

If Organization decides to follow security industry best practices like SOC2, will follow an Incident Response Plan and test this plan annually. If any updates are needed, the plan will be updated and approved.

Employees can report suspected incidents to their supervisor, the Security Officer or use Organization's reporting tool.

Incident Management

Identification and Determination of Security incidents

Incident Detection and Identification Incidents can be detected through existing logging and monitoring controls, receiving reports from personnel or the public, or running into an operational disruption or problem. Suspected incidents should be documented in Organization's ticketing system or similar tracking mechanism and triaged by the appropriate team.

Once an incident has been triaged and confirmed, attempts should be made to identify the type of incident, if possible. The identification process may take some investigation and collaboration across business units.

At this time, the Security Official must be notified if the incident affects PHI or ePHI for further action. The Security Official will contact the Privacy Official and collaborate to respond to the incident. Organization may need to consult with legal counsel if the incident calls for it. Security incidents that involve ePHI need to be handled in a specific way and have additional responses, like breach determinations and notifications. Refer to the Data Security Policy– HIPAA Incident Response, Reporting, and Breach Determination to handle Security Incidents involving ePHI*.*

While the supervisor or Security Official takes appropriate actions, Organization will avoid making any updates or other modifications to software, data, or equipment involved in the incident. This preserves evidence if further investigation is needed.

Incident Documentation

Organization documents each incident through to completion. Documentation of an incident should include details like:

- When the incident occurred and for how long
- What caused the incident
- How widespread the vulnerability is
- What Organization did to respond to the incident
- How the incident was resolved

- Lessons learned from the incident

Examples of details to include are:

- Hardware address
- System name
- IP address
- *ePHI* data processed by the system
- Applications installed on the system
- Location of the system

Organization will also document which systems were impacted, and what access was used, if possible.

The Incident management module in the Guard can be used to document incident and incident response including investigations.

Incident Response

Incidents come in many forms and may require different response approaches. In order to respond to an incident, Organization will convene an Incident Response Team (IRT) to tackle the incident, exept for those involving ePHI will be handled under the Data Security Policy– HIPAA Incident Response, Reporting, and Breach Determination. The IRT will then begin incident response using the *Incident Response Plan.*

Incident Response Plan

When responding to an incident, the IRT must perform and document the following:

- Investigation of the incident, including determining root cause
- Measures taken to contain the incident
- Eradication of the incident, which can include:
- Deletion, removal, or replacement of malicious or infected files
- Modification, re-creation, or termination of user accounts, if there is evidence of unauthorized access
- Restoration from a clean backup

- Incident recovery, which can include:
- Restoring data from a clean backup
- Bringing systems back online
- Enabling user access and accounts
- The IRT must document lessons learned from the incident and work with Organization to adopt any improvements that are necessary.

The *Incident Response Plan* will be tested annually and updated as needed.

ROLES AND RESPONSIBILITIES

Security Officer: Coordinates with Privacy Officer to address any incidents that affect PHI or ePHI. Determines if any laws or regulations may have been violated.

Incident Response Team (IRT): Team(s) responsible for responding to other security incidents.

VIOLATIONS

Organization may take disciplinary action should evidence show that an internal user caused or contributed to the incident.

RELATED FORMS/PLANS/DOCUMENTS

- Incident Response Plan

RELATED POLICIES AND PROCEDURES

- Data Security – Incident Response and Reporting Procedure
- Data Security – HIPAA Incident Response, Reporting, and Breach Determination
- Breach Notification Policy

RELEVANT HIPAA REGULATIONS

- § 164.308(a)(6)(i) *Security incident procedures*
- § 164.308(a)(6)(ii) *Response and reporting*

RELEVANT SOC 2 CRITERIA

- CC 7.3.1 *Responds to Security Incidents*
- CC 7.3.2 *Communicates and Reviews Detected Security Events*

- CC 7.3.3 *Develops and Implements Procedures to Analyze Security Incidents*
- CC 7.3.4 *Assesses the Impact on Personal Information*
- CC 7.3.5 *Determines Personal Information Used or Disclosed*
- CC 7.4.1 *Assigns Roles and Responsibilities*
- CC 7.4.2 *Contains Security Incidents*
- CC 7.4.3 *Mitigates Ongoing Security Incidents*
- CC 7.4.4 *Ends Threats Posed by Security Incidents*
- CC 7.4.5 *Restores Operations*
- CC 7.4.6 *Develops and Implements Communication Protocols for Security Incidents*
- CC 7.4.7 *Obtains Understanding of Nature of Incident and Determines Containment Strategy*
- CC 7.4.10 *Evaluates the Effectiveness of Incident Response*
- CC 7.4.11 *Periodically Evaluates incidents*
- CC 7.4.12 *Communicates Unauthorized Use and Disclosure*
- CC 7.4.13 *Application of Sanctions*

Data Security Policy - Information Access Management

PURPOSE

To provide principles and guidelines for information access management at Organization, including access to ePHI.

SCOPE

The Information Access Management Policy will cover Organization's**:**

- Information access management, including sensitive and protected information, such as ePHI

- Identity, roles, and authorization of user access to sensitive and protected information, such as ePHI
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY/PROCEDURES

Organization has and follows policies and procedures for managing access to information, including sensitive and protected information, like ePHI*.* Physical access to sensitive or protected information is also considered. The company considers access in the context of regulatory and compliance obligations, such as the HIPAA Security Rule.

Organization applies principles of "least privilege" and role-based access control throughout its operations and restricts access to sensitive and protected information and systems on a need-to-access basis. Access to systems and data is tied to users' identities.

Organization has set up systems and processes to record access requests, approvals, provisioning, modification, and termination. These Access Controls are captured in our *Access Control Policy*.

Access Reviews

Organization reviews access on a regular basis, including access to ePHI and other sensitive data. If changes are required based on the access review, they are carried out in a timely manner.

ROLES AND RESPONSIBILITIES

Security Official: Accountable for user access to ePHI and other protected data*.*

VIOLATIONS

Inappropriately accessing sensitive or protected data may result in disciplinary action, in compliance with the HIPAA Security Rule.

FORMS/PLANS/DOCUMENTS

- Onboarding Checklist
- Offboarding Checklist
- Access Reviews
- User Access Listing or Population

RELATED POLICIES AND PROCEDURES

- Data Security – Access Control Policy

RELEVANT HIPAA REGULATIONS

- §164.308(a)(4)(i) *Information Access management*
- §164.308(a)(4)(ii)(B) *Access authorization*
- §164.308(a)(4)(ii)(C) *Access establishment and modification*

RELEVANT SOC 2 CRITERIA

- CC5.2.3 *Establishes relevant technology infrastructure control activities*
- CC6.2.1 *Controls access credentials to protected assets*
- CC6.2.2 *Removes access to protected assets when appropriate*
- CC6.2.3 *Reviews appropriateness of access credentials*
- CC6.3.1*Creates or modifies access to protected information assets*
- CC6.3.2 *Removes access to protected information assets*
- CC6.3.3 *Uses role-based access controls*

Data Security Policy – Integrity Control

PURPOSE

To provide principles and guidelines for information and system integrity control.

SCOPE

The Integrity Control Policy will cover Organization's:

- Data, information, and system integrity controls
- Detection of unauthorized changes or destruction of data
- Roles and Responsibilities

- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY

Organization has adopted and follows processes to safeguard the integrity of sensitive and protected information, such as ePHI. These security measures are designed to protect information and systems from unauthorized modification, deletion, or access.

Organization has set up processes for detecting unauthorized changes or destruction of information and data. These processes may include mechanisms for validating the integrity of data. If an anomaly or event is detected, workforce members should report the event. Detection mechanisms are periodically reviewed and tuned to optimize operations.

PROCEDURES

Organization has set up processes to safeguard the integrity of sensitive and protected information, including ePHI.

Data, Information, and System Integrity Controls

In order to maintain the integrity of the company's production environment, Organization has set up separate production, development, and test environments. Only tested and approved components, infrastructure, and information is migrated or released into production. By separating environments, Organization can better ensure that only thoroughly validated systems, components, and data appear in production. To further safeguard sensitive and protected information, only "dummy data" or non-production data will be used in development and test environments.

Organization has set up strong encryption and cryptographic security on sensitive and protected information, including *ePHI*, at-rest and in-transit. The company uses modern, secure algorithms to encrypt sensitive or protected data.

Detection of Unauthorized Changes or Destruction of Data

Organization uses a combination of electronic authentication, procedural authentication, and data and system integrity checks to detect and protect *ePHI* from unauthorized changes, destruction, or disclosure.

Workforce members are trained and encouraged to report any suspected unauthorized access, changes, deletion, or disclosure of sensitive or protected information, including *ePHI*.

Organization has set up automated alerting mechanisms and filters to analyze anomalies and alert on potential threats to data or system integrity. These alerts are routed through the company's incident response and reporting procedure.

Definitions

Electronic Authentication - Mechanisms such as error-correcting memory, digital signatures, and checksum technology used to check data or system integrity.

Procedural Authentication - Mechanisms such as manual validation used to check data or system integrity.

Data and System Integrity Checks - Mechanisms and procedures (e.g., backup verification, hardware and software reviews) to perform periodic checks of data and system functionality to identify *integrity* issues (e.g., corrupted data, failing hardware, software errors).

RELEVANT HIPAA REGULATIONS

- 164.312(c) *Mechanism to Authenticate Electronic Protected Health Information*

RELEVANT SOC 2 CRITERIA

- CC6.8.2 *Detects unauthorized changes to software and configuration parameters*
- CC7.2.1 *Implements detection policies, procedures, and tools*
- CC7.2.2 *Designs detection measures*
- CC7.2.3 *Implements filters to analyze anomalies*
- CC7.2.4 *Monitors detection tools for effective operation*
- CC7.3.2 *Communicates and reviews detected security events*

Data Security Policy – Monitoring and Effectiveness

PURPOSE

To provide principles and guidelines for performing regular security assessments and monitoring of Organization's data security program. To provide detailed instructions for conducting regular security assessments and monitoring of Organization's data security program.

SCOPE

The Monitoring and Effectiveness Policy and Procedures will cover Organization's:

- Security assessments and process, including
- Technical and non-technical assessments

- Remediation
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY

Organization conducts regular security assessments to evaluate the effectiveness of our data security program. These security assessments will also be performed in the event of a major change.

Assessments can be performed by both internal and external parties.

Assessment reports are communicated to company leadership and the Board of Directors.

Technical and Non-Technical Assessments

Organization uses a mix of technical and non-technical assessments to monitor the effectiveness of our data security program. Assessments may include penetration testing, risk assessments and audits and can include use of the Guard's Data Security Program.

Remediation

Any findings resulting from security assessments will be documented and tracked in a risk register. The Guard's data security program can be used to accomplish this. We develop action plans to address these issues, and track remediation to completion.

PROCEDURES

Organization conducts security assessments **annually** and uses a mix of technical and non-technical measures to evaluate the effectiveness of our data security program. Additional assessments are performed when major changes occur that call for a formal security assessment.

Organization works with its internal teams and third parties to conduct security assessments. Any third parties that are contracted to perform security assessments must meet our due diligence and third-party risk requirements. We may use the Data Security and Physical Safeguards Programs in The Guard to accomplish this.

The results from security assessments are documents and communicated to company leadership, including the Board of Directors when appropriate.

Technical and Non-Technical Assessments

Organization performs penetration testing or an equivalent technical assessment on an annual basis to evaluate our data security program. Technical assessments should cover:

- ePHI and other sensitive information security and controls

- Key information systems
- Security configurations
- Infrastructure security
- Network security
- Application security
- Workstation/Endpoint security
- Identification of new or emerging technology risks

Non-technical assessments should evaluate:

- The overall information security program and controls, including:
    -
    - Access controls
    - Audit controls
    - Integrity controls
    - Identity and authentication controls
    - Incident response controls
    - Contingency planning controls
- The effectiveness of controls to mitigate risks
- Identification of new or emerging business risks
- Facility and physical security controls

All assessments are documented. New risks are logged in our risk register. The Guard's program module can be used to accomplish this for the non-technical assessments and as an evidence collection tool for the technical assessments.

Remediation

Any findings, observations, or issues discovered over the course of a security assessment should be logged in our risk register. Organization will update its security measures to remediate issues identified during an assessment. These updates will be reflected in updated policies and

procedures. Remediation efforts should reduce the likelihood or impact of an identified risk to an acceptable level.

Remediation will be tracked to completion. This can be accomplished by adding, tracking and completing tasks attached to the relevant controls in the Guard's Data Security and Physical Safeguard Programs.

ROLES AND RESPONSIBILITIES

Security Assessor(s): Conducts technical and non-technical security assessments. Records risks, observations, and findings and reports them to management. Provides remediation recommendations.

FORMS/PLANS/DOCUMENTS

- Security Assessment Report(s)
- Risk Register

RELEVANT HIPAA REGULATIONS

- § 164.308(a)(8) *Perform a periodic technical and non-technical evaluation.*

RELEVANT SOC 2 CRITERIA

- CC 2.3.3 *Communicates With the Board of Directors*
- CC 3.4.4 *Assess Changes in Systems and Technology*
- CC 4.1.1 *Considers a Mix of Ongoing and Separate Evaluations*
- CC 4.1.2 *Considers Rate of Change*
- CC 4.1.3 *Establishes Baseline Understanding*
- CC 4.1.4 *Uses Knowledgeable Personnel*
- CC 4.1.5 *Integrates With Business Processes*
- CC 4.1.6 *Adjusts Scope and Frequency*
- CC 4.1.7 *Objectively Evaluates*
- CC 4.1.8 *Considers Different Types of Ongoing and Separate Evaluations*
- CC 4.2.1 *Assesses Results*

- CC 4.2.2 *Communicates Deficiencies*
- CC 4.2.3 *Monitors Corrective Action*

Data Security Policy – Policy and Procedure Management

PURPOSE

To provide principles and guidelines for managing policies, procedures, and other documentation at Organization.

SCOPE

The Policy and Procedure Management document will cover Organization's:

- Policy and procedure review
- Compliance documentation, access, and retention
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY/PROCEDURES

Organization's Security Officer is responsible for implementing policies and procedures that meet the requirements of the HIPAA Security Rule.

All policies and procedures related to the HIPAA Security Rule and other regulatory and compliance standards followed by the company are written and retained, usually in electronic form. Related documentation is also created and retained for security measures and control activities.

Documentation is retained for a minimum of six (6) years from the time of its creation or the date it was last in effect, whichever is later.

Access to security and compliance documentation other than policies and procedures is limited only to those people who require access for their job functions and/or roles.

Policies and procedures, as well as other key documents, are reviewed at least annually and updated as needed. Reviews of policies and procedures must include the date of review, and the signoff of the reviewer.

ROLES AND RESPONSIBILITIES

Security Official: Responsible for adopting policies and procedures that meet the requirements of the HIPAA Security Rule for the company.

Policy Owner or Reviewer: Responsible for reviewing and updating policies and/or procedures that fall under their jurisdiction.

RELEVANT HIPAA REGULATIONS

- §164.316(a) Policies *and procedures*
- §164.316(b)(1) *Documentation*
- §164.316(b)(2)(i)*Time limit*
- §164.316(b)(2)(ii) *Availability*
- §164.316(b)(2)(iii) *Updates*

RELEVANT SOC 2 CRITERIA

- CC5.3.2 *Establishes responsibility and accountability for executing policies and procedures*

Data Security Policy - Security Awareness and Training

PURPOSE

To provide rules for security awareness and training for members of the workforce, including management.

SCOPE

The Security Awareness and Training Policy and Procedure will cover:

- Security updates and reminders
- Security training for employees;
- Security awareness and training process, including
- Malware Training

- Social Engineering Training
- Password creation, modification, and protection
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- And Relevant Regulations, Standards, and Criteria.

POLICY

Fostering security awareness and providing training for Organization's employees is key to protecting Organization from security threats and accidental errors. Organization wants to foster a security-aware culture.

Organization has adopted and followed a security awareness and training program for all members of the workforce (including management). Organization will require employees to complete security training in The Guard. Trainees will need to acknowledge that they completed and understood the training, and Organization will document all attestations.

Security Updates

To foster a security-aware culture, Organization will provide periodic security updates to the workforce, covering topics including:

- Security threats to ePHI that recently occurred or may occur
- Changes to Organization's security program, policies, technologies, or procedures
- The importance of security to HIPAA and other regulatory and compliance efforts
- And other security updates relevant to the workforce

Organization may opt to use email newsletters, videos, webinars, and other forms of media or communications to provide security updates to the workforce.

Security Training

As part of Organization's security awareness and training program, we will provide security training to employees upon hire and annually. Employees, including management, are required to complete security training and acknowledge that they have completed training. Training logs need to be retained for compliance purposes.

Social Engineering Training

Social engineering attempts, including phishing, involve using a fake communication, like an email, phone call, or text message, to trick users into providing a bad actor with confidential data or passwords. This is a common attack vector used by cybercriminals to breach organizations

today, and Organization provides employees with training to identify and respond to potential social engineering attempts.

Password Management Training

Creating and protecting passwords and secrets can make all the difference in security.

Organization's security training will provide employees with instructions on creating and protecting strong passwords.

PROCEDURES

Organization will review and update this Security Awareness and Training Policy and Procedure at least annually.

If Organization determines that additional training is required for a subset of workforce members, such as system owners and administrators, the company will make those resources available.

Workforce members who fail to demonstrate a clear understanding of security awareness may be required to complete additional or supplemental training.

Security Updates

Organization sends security updates to employees at least quarterly via company email. The company will post signs and reminders in physical workspaces to remind employees about security best practices.

Security Training

Organization's Security Training includes:

- Information on Organization's security policies, procedures, and technologies
- Procedures for protecting company devices from malicious software, including:
    -
        - Potential harm that can be caused by malware
        - Malware prevention, and how malware prevention software works
        - What to do in the event of a malware infection
        - How to report a potential malware infection
- Procedures for handling social engineering attempts
    -
        - Ways to identify suspicious emails, texts, and communications

    - What to do if targeted by a phishing or social engineering attack
    - How to report a potential attack attempt
- Procedures for creating strong passwords and safeguarding secrets
- Policy and Procedure for Incident Response and Reporting
- Policy and Procedure for Workstation Use and Workstation Security
- Changes to Organization's security program
- Other security topics relevant to Organization

You may use The Guard's Training and Policy Modules and materials to achieve these control objectives.

Freshness of Security Awareness Training
Organization will ensure that all new members of the workforce receive security awareness training on hire and on at least an annual basis.

RELEVANT HIPAA REGULATIONS:

- §164.308(a)(5)(i) *Security awareness and training*
- §164.308(a)(5)(ii)(A) *Security reminders*
- §164.308(a)(5)(ii)(B) *Protection from malicious software*
- §164.308(a)(5)(ii)(C) *Log-in monitoring*
- §164.308(a)(5)(ii)(D) *Password management*

RELEVANT SOC 2 CRITERIA:

- CC 1.4.3: *Attracts, develops, and retains individuals.*
- CC 1.4.7: *Provides training to maintain technical competencies.*
- CC 2.2.6: *Communicates information on reporting failures, incidents, concerns, and other matters.*
- CC 2.2.8: *Communicates information to improve security knowledge and awareness.*
- CC 2.3.6: *Communicates objectives related to confidentiality and changes to objectives.*

- CC 2.3.11: *Communicates information on reporting system failures, incidents concerns, and other matters.*

- CC 6.7.1: *Restricts the ability to perform transmission.*

- CC 6.7.2: *Uses encryption technologies or secure communication channels to protect data.*

- CC 6.7.3: *Protects removal media.*

- CC 6.7.4: *Protects mobile devices.*

APPENDIX A: PASSWORD SECURITY BEST PRACTICES

NIST recommends the following password standards for creating strong passwords:

- Use a minimum of eight (8) characters, with longer passwords being more secure

- Disallow or do not use sequences or repetitive characters, such as “12345” or “aaaaa”

- Disallow or do not use context-specific passwords, like the name of the site or company

- Disallow or do not use commonly used passwords, such as “password123” and “12345678”

- Disallow or do not use single dictionary words

- Disallow or do not use passwords that have been compromised previously

In addition, the company encourages the following password best practices:

- Do not share passwords with others

- If you suspect that your password has been compromised, change your password immediately and report the incident

- Do not reveal passwords over the phone or via email

- Do not provide password hints

- Do not use another user’s username and password

- Do not write down usernames and passwords

Data Security Policy – Security Management

PURPOSE

To provide principles and guidelines for managing Organization's information security program and processes.

SCOPE

The Security Management Policy will cover Organization's:

- Information Security Management policy and program
- Security program documentation, including creation and retention
- Organizational structure
- Risk management activities, treatment, and assessments
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY

Organization has defined a security management process that incorporates a risk-based approach, and takes into account the resources, both internal and external, available to the company. Organization considers information security a priority and has established controls and processes to keep sensitive information and protected information, such as ePHI, safe.

In addition to specific processes and controls, Organization's leadership, including senior management and the Board of Directors, are committed to a security-conscious company culture, and information security.

Information Security Management Program

Organization's information security program defines roles and responsibilities for personnel. Charts, policies, and procedures reflect the responsibilities of the Board of Directors, the independence of the Board, and the expertise available on the Board.

Organization has based its information security program on frameworks and best practices that support its objectives, including relevant accounting standards and the Center for Information

Security (CIS). The company's information security program considers the regulatory and compliance standards that need to be included in the program, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Organization's information security program ensures that controls and processes maintain the confidentiality, integrity, and availability (the CIA triad) of sensitive or protected data. When needed, the company separates incompatible duties between different personnel or roles.

Organization Chart
Organization has an organization chart that lists personnel and their roles and/or titles and includes reporting lines. The organization chart is reviewed and updated at least annually, or when significant changes occur.

Compliance Documentation and Retention
For compliance and analysis purposes, all control activities related to information security are documented. This documentation may need to be provided for audit and assessment purposes. Documentation is a key step in any control activity and should always be completed thoroughly. Electronic documentation, audit logs, ticketing systems, and other IT systems assist with collecting this type of documentation and information. Access to documentation repositories is limited to appropriate personnel only, as it may contain sensitive or protected information.

Risk Management
Organization applies risk management principles to its information security program in order to better identify, assess, and address risks or threats to the company. Information security risk management involves a cycle of steps:

1. Risk Identification
2. Risk Analysis
3. Risk Treatment and Action Plan
4. Risk Monitoring and Review

Risk assessments are an important part of our risk management program and are performed at least annually. The Guard's data security program is available as one tool in this assessment and includes evidence collection and risk assessment components.

The company's risk register is also reviewed and updated at least annually and includes any findings from completed risk assessments.

Risk Register
A risk register is a document or database that contains a listing of the company's risks, including:

- Risk description

- Risk likelihood score
- Risk impact score
- Risk analysis (aggregated score, usually calculated as likelihood score * impact score)
- Risk treatment
- Risk action plan or remediation plan, including an estimated date of completion
- Risk owner
- Other relevant notes or data points

Risk Committee
Organization has created a Risk Committee and an accompanying Charter that outlines the Risk Committee's purpose, objectives, and required deliverables or outcomes. The Risk Committee meets at least quarterly, and documents meeting minutes that we retain for compliance purposes. If necessary, the risk register should be updated to reflect updates and changes following the Risk Committee meeting.

ROLES AND RESPONSIBILITIES
Risk Committee: Meets quarterly to review the company's risk posture, including the risk register and any recent risk assessments. Provides cross-functional insights into risk management. Decides the priority of risks as needed.

VIOLATIONS
Violations of the information security policy and program may be subject to disciplinary action.

FORMS/PLANS/DOCUMENTS
- Organization Chart
- Risk Committee Charter
- Risk Committee Meeting Minutes
- Risk Assessment Documentation

RELEVANT HIPAA REGULATIONS
- [§164.308(a)(1)(ii)(A)](https://www.ecfr.gov/cgi-bin/text-idx?node=pt45.2.164&rgn=div5
Risk analysis

- [§164.308(a)(1)(ii)(B)](https://www.ecfr.gov/cgi-bin/text-idx?node=pt45.2.164&rgn=div5 *Risk management*

- [§164.308(a)(1)(ii)(C)](https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164 *Sanctions Policy*

- [§164.308(a)(1)(ii)(D)](https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164 *Information system Activity Review*

RELEVANT SOC 2 CRITERIA

- CC1.1.1 *Sets the tone at the top*

- CC1.2.1 *Establishes oversight responsibilities*

- CC1.2.2 *Applies relevant expertise*

- CC1.2.3 *Operates independently*

- CC1.2.4 *Supplements board expertise*

- CC1.3.1 *Considers all structures of the entity*

- CC1.3.2 *Establishes reporting lines*

- CC1.3.3 *Defines, assigns, and limits authorities and responsibilities*

- CC1.3.4 *Addresses specific requirements when defining authorities and responsibilities*

- CC3.1.1 *Reflects management's choices*

- CC3.1.2 *Considers tolerances for risk*

- CC3.1.3 *Includes operations and financial performance goals*

- CC3.1.4 *Forms a basis for committing of resources*

- CC3.1.5 *Complies with applicable accounting standards*

- CC3.1.6 *Considers materiality*

- CC3.1.7 *Reflects entity activities*

- CC3.1.8 *Complies with externally established frameworks*

- CC3.1.9 *Considers the required level of precision*

- CC3.1.10 *Reflects entity activities*
- CC3.1.11 *Reflects management's choices*
- CC3.1.12 *Considers the required level of precision*
- CC3.1.13 *Reflects entity activities*
- CC3.1.14 *Reflects external laws and regulations*
- CC3.1.15 *Considers tolerances for risk*
- CC3.1.16 *Establishes sub-objectives to support objectives*
- CC4.2.1 *Assesses results*
- CC4.2.2 *Communicates deficiencies*
- CC5.1.1 *Integrates with risk assessment*
- CC5.1.2 *Considers entity-specific factors*
- CC5.1.3 *Determines relevant business processes*
- CC5.1.4 *Evaluates a mix of control activity types*
- CC5.1.5 *Considers at what level activities are applied*
- CC5.1.6 *Addresses segregation of duties*
- CC5.3.1 *Establishes policies and procedures to support deployment of management's directives*
- CC5.3.2 *Establishes responsibility and accountability for executing policies and procedures*

Data Security Policy – Transmission Security

PURPOSE

To provide principles and guidelines for protecting data-in-transit and secure data transmission.

SCOPE

The Transmission Security Policy will cover Organization's:

- Data transmission safeguards
- Secure data transmission
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY

Organization has adopted and follows security measures to protect the confidentiality and integrity of sensitive and protected information, such as ePHI, that is transmitted over a network.

Any sensitive or protected data transmitted over a network must be protected from unauthorized access or disclosure. Data transmission safeguards must also prevent modification or corruption, or alert in the event of data modification or corruption.

Organization requires the following security measures for sensitive or protected data-in-transit, including ePHI:

- Sensitive or protected data, including ePHI, must be securely encrypted during transmission unless explicitly requested in writing by the patient
- Remote access to ePHI must be secure, such as over a Virtual Private Network (VPN)
- End-to-end email encryption

Encryption methods used to protect data-in-transit should be up-to-date and secure, such as TLS 1.2+.

Employees must avoid sending ePHI and other sensitive or protected information through insecure or unapproved mechanisms except in very limited circumstances as required under HIPAA upon the request of an individual. In those instances, transmission should only be after consultation with the security officer.

PROCEDURES

Organization requires certain controls and safeguards for the transmission of sensitive or protected data or information over a network. The company requires all data-in-transit to be encrypted and use secure protocols, such as TLS1.2+.

Remote access to ePHI is only permitted through a VPN or other approved secure connection mechanism.

ePHI will not be sent over unencrypted email unless explicitly requested in writing by the patient. Patients requesting unencrypted ePHI over email should be informed that this is not a secure method of communication. Any ePHI sent via email should be redacted in replies.

Workforce members are prohibited from sending ePHI and other sensitive or protected information using insecure or unapproved methods except in very limited circumstances as required under HIPAA upon the request of an individual. In those instances, transmission should only be after consultation with the security officer.

Encryption
Organization has set up processes and safeguards to encrypt

- Data-at-rest
- Data-in-transit
- Files, data, and devices that store or process sensitive or protected information, including ePHI
- Emails containing ePHI
- Other devices, disks, and systems

RELEVANT HIPAA REGULATIONS

- §164.312(e)(1) *Transmission security*
- §164.312(e)(2)(i) *Integrity controls*
- §164.312(e)(2)(ii) *Encryption*

RELEVANT SOC 2 CRITERIA

- CC6.1.2 *Restricts logical access*
- CC6.6.2 *Protects identification and authentication credentials*
- CC6.7.1 *Restricts the ability to perform transmission*
- CC6.7.2 *Uses encryption technologies or secure communication channels to protect data*
- CC6.8.5 *Scans information assets from outside the entity for malware and other unauthorized software*

Data Security Policy - Workforce Security

PURPOSE
To provide principles and guidelines for managing the workforce and workforce security.

SCOPE
The Workforce Security Policy and Procedure will cover Organization's**:**

- Workforce security
- Job descriptions
- Workforce background checks or screenings
- Confidentiality agreements
- Development and performance reviews
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY
Organization has adopted and follows processes to enforce workforce security and workforce management controls. The company restricts access to sensitive and protected information, including ePHI, to appropriate and authorized members of the workforce only. When necessary, Organization sets up controls to separate incompatible duties and responsibilities.

The company has set up workflows to supervise the approval of access to sensitive and protected information and assets.

Organization aims to foster a security-conscious workforce and culture and seeks to hire, develop, and maintain skilled workforce members.

Job or Role Descriptions
To attract and hire skilled talent, Organization requires written and defined job or role descriptions for each position at the company, and for recruitment. Job descriptions should be periodically reviewed and updated when necessary.

Workforce Background Checks and Security Screenings

As part of the recruitment process, the company has adopted and follows a defined screening process, incorporating interviews, case studies, or technical examinations when appropriate for the job or role.

Organization requires a background check to be performed when possible prior to hiring an employee. If a background check is not possible due to privacy laws, the company will use a different screening method.

Development and Performance Reviews

Developing the workforce is key to Organization's success. Organization provides basic security training for all employees and provides role- or job-specific training as needed.

The company provides resources for employees' development and completes a regular performance review for all employees. Performance reviews should be documented and follow a defined process.

Confidentiality Agreements

Prior to beginning work, workforce members must sign Organization's Confidentiality Agreement. While not required for HIPAA compliance, it is a best practice.

PROCEDURES

Job Or Role Descriptions

Whenever a new role or job is opened, a formal job description is created and maintained. Job descriptions should be reviewed at least annually and updated if necessary.

Workforce Background Checks and Security Screenings

Organization uses various screening mechanisms, such as interviews, case studies, or technical examinations to evaluate applicants for a job function or role. All new hires must have a background check completed prior to onboarding. If a background check is not permitted due to regional laws or mandates, the company will use a combination of background screening methods, such as references and work experience.

Screening records and background check documentation is retained for compliance purposes. The company may redact information on screening records and background check documentation when appropriate.

Development and Performance Reviews

To attract, retain, and develop workforce members, Organization requires all employees to undergo basic security training that covers proper handling and protection of PHI and *ePHI*. The company provides role- and job-specific training to employees and workforce members as needed.

At least annually, Organization completes a performance review for all employees. Performance reviews should be documented and retained, including information about the individuals involved in the review, the date the review was performed, and any action items or outcomes resulting from the review. These performance reviews will be kept as part of workforce records.

Confidentiality Agreements

Organization requires all workforce members, including contractors, to sign a Confidentiality Agreement. These Confidentiality Agreements are retained as part of workforce records. This can be accomplished using the Guard's Vendor module or by other similar means.

ROLES AND RESPONSIBILITIES

Security Official: Accountable for workforce security and workforce access to sensitive and protected information, including *ePHI.* Delegates responsibilities and authority as needed. Informs workforce members of changes to access levels or clearance or delegates these communications.

Access Approval: Delegates with appropriate levels of knowledge and experience may have access approval authority for certain roles, information, assets, and/or systems. Access requests that require approval may be routed to one or more supervisory approvers.

VIOLATIONS

Access to information or assets may be revoked or suspended if a workforce member has accessed sensitive or protected information without the right level of authorization and approval.

FORMS/PLANS/DOCUMENTS

- Confidentiality Agreement (Samples available in the Guard Document Module)
- Offboarding Checklist

RELATED POLICY

- Data Security Policy - Access Control

RELEVANT HIPAA REGULATIONS

- §164.308(a)(3)(i) *Workforce security*
- §164.308(a)(3)(ii)(A) *Authorization and/or supervision*
- §164.308(a)(3)(ii)(B) *Workforce clearance procedure*
- §164.308(a)(3)(ii)(C) *Termination procedures*

RELEVANT SOC 2 CRITERIA

- CC5.2.3 *Establishes relevant technology infrastructure control activities*
- CC6.1.2 *Restricts logical access*
- CC6.1.6 *Restricts access to information assets*

- CC6.2.1 *Controls access credentials to protected assets*
- CC6.2.3 *Reviews appropriateness of access credentials*
- CC6.3.3 *Uses role-based access controls*
- CC6.1.8 *Manages credentials for infrastructure and software*

Data Security Policy – Workstation Use and Workstation Security

PURPOSE

To provide principles and guidelines for the secure use of workstations by **Organization's** workforce. To provide detailed instructions for the secure configuration and use of workstations by **Organization's** workforce.

SCOPE

The Workstation Use and Workstation Security Policy and Procedures cover Organization's requirements for**:**

- Workstation use
- Workstation security, including
    -
    - Workstation access control
    - Workstation physical security
    - Secure workstation configurations
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY

Organization defines workstations as the endpoint devices, such as computers, tablets, or mobile phones, that employees use to conduct their job duties. For on-site workers, this includes their workspace, cubicle, and desk area.

Organization adopts and follows workstation use and security controls that support the confidentiality, availability, and integrity of ePHI and other sensitive information.

Organization catalogs all devices in our IT environment in our asset inventory.

Workstation Use

Employees should only use company-issued or approved assets for their job role and related responsibilities. Only appropriate personnel have access to ePHI or other sensitive information, as required by their role.

Organization requires employees to keep ePHI and other sensitive information secure and prevent unauthorized personnel from viewing or obtaining that information.

Physical Workstation Use

Organization adopts and follows processes that keep workstations, ePHI, and other sensitive information physically secure.

Remote Workstation Use

Temporary, hybrid, and fully remote workers must use secure channels, such as VPN, to access ePHI when they are not at a company facility.

Workstation Security

Organization adopts and follows processes that safeguard workstations with access to ePHI or other sensitive information.

We do not allow the use of removable media, such as USB drives, external hard drives, or SD cards.

Workstation Access Control

Organization adopts and follows processes for restricting access to workstations with access to ePHI or other sensitive information.

Secure Workstation Configurations

Organization has set up workstation configuration baselines in order to protect confidential information. All workstations must meet the workstation configuration baseline to be used for work. These workstation configurations include session timeout, password requirements, and regular anti-virus/anti-malware scans.

PROCEDURES

Organization adopts and follows processes for workstation use and workstation security that support the confidentiality, availability, and integrity of *ePHI* and other sensitive information.

All workstation devices are logged in our asset inventory with the following details:

- Asset tag (highly recommended)
- Unique ID or Serial Number
- Device Name
- Device Type
- Operating System and Version
- Assignee or Device Owner
- IP Address (most recent)
- MAC Address

Workstation Use

Organization's workforce members agree to use company assets and devices for appropriate purposes only. Workforce members should only access ePHI and sensitive information through authorized devices.

Organization does not allow the use of removable media for storing ePHI and other sensitive information.

Workforce Members have *no expectation of privacy* when using Organization's company assets and devices.

Physical Workstation Use

Employees must take measures to prevent unauthorized access to *ePHI* and other sensitive information, including making sure that screens are protected from view, such as through a privacy screen. When transporting endpoint devices, workforce members should keep them locked and out of sight in their vehicles. Passwords should never be written down in an accessible location or kept on a post-it note on your workstation.

Any PHI or sensitive information in physical form must be locked away when not in use. All PHI or sensitive information must be securely destroyed. Physical keys should also be secured and kept out of sight.

Mobile endpoint devices should be locked away in a cabinet or drawer when unattended.

Remote Workstation Use

Workforce members who work remotely must maintain a secure work environment and safeguard ePHI and other sensitive information from unauthorized access.

Workforce members must use VPN or an equivalent secure channel to access ePHI and other sensitive information when working remotely.

Workstation Security

Organization adopts and follows processes for configuring and securing workstations and restricting access to workstations with access to ePHI or other sensitive information.

Workstations are placed in secure locations and to prevent unauthorized individuals from viewing device screens or confidential data.

Workstation Access Control

Individuals receive unique IDs and credentials for logging into workstations. Users must create strong passwords that align with Organization's password requirements.

Users are not allowed to share their credentials with other users.

Secure Workstation Configurations

Organization has set up and defined workstation configuration baselines to protect confidential information and workstation security. All workstations issued by the company are required to meet the workstation configuration baselines. Employees should not tamper with secure workstation configurations.

Organization requires these secure configurations for all company-issued workstations and/or devices:

- **Password Protection:** Endpoint devices must be secured with strong passwords that enforce Organization's password requirements.

- **Anti-Virus and Anti-Malware:** AV/AM software must be installed on all endpoint devices and be scheduled to run and remove malicious software on a weekly basis at minimum.

- **Session Timeout:** Endpoint devices will lock out the session after a set time of inactivity (best practice is <15 minutes). Users must log back into devices using their credentials.

- **Deny Auto-Run:** Endpoint devices should be prohibited from auto-running removable media.

- **Encryption:** Endpoint devices should be encrypted by default.

Organization manages our endpoints and devices using a mobile device management (MDM) solution when appropriate or feasible.

ROLES AND RESPONSIBILITIES

IT Team or IT Manager: Securely configures workstations based on the workstation configuration baseline(s). Issues company devices and workstations. Troubleshoots workstations.

VIOLATIONS

Employees that knowingly disable security controls or circumvent workstation controls may face disciplinary action.

Allowing unauthorized access to ePHI and other sensitive information can lead to disciplinary action, up to and including termination.

FORMS/PLANS/DOCUMENTS

- Workstation Secure Configuration Baseline
- Asset Inventory
- Workstation Use Policy or Acceptable Use Policy

RELEVANT HIPAA REGULATIONS

- [§164.310(b)] https://www.law.cornell.edu/cfr/text/45/164.310 *Workstation use*
- [§164.310(c)] https://www.law.cornell.edu/cfr/text/45/164.310 *Workstation security*

RELEVANT SOC 2 CRITERIA

- CC 6.1.3 *Identifies and Authenticates Users*
- CC 6.1.5 *Manages Points of Access*
- CC 6.7.3 *Protects Removal Media*
- CC 6.7.4 *Protects Mobile Devices*
- CC 6.8.4 *Uses Anti-Virus and Anti-Malware Software*