Reviewed:11/18/2022

HIPAA SECURITY POLICY AND PROCEDURE MANUAL

Company Name: Will be referred to as [Organization] throughout each policy in this manual	**Advanced Metrics**
Policy Name:	Security Policy
Policy Version:	Version 2.0
Effective Date:	**11/18/2022**
Review Date:	Yearly
Security Official: Will be referred as Security Official throughout each policy.	**John Kreiner**
Privacy Official: Will be referred as Privacy Official throughout each policy.	**Martha Shetrompf**
Compliance Official: Will be referred as Compliance Official throughout each policy.	**Steven Herr**
Responsible for Review:	**Martha Shetrompf**

Table of Contents

Confidentiality Agreement

As a *workforce member* of **Organization**, I understand that **Organization**, a covered entity under the HIPAA regulations, has a legal responsibility to protect the privacy and security of patient Protected Health Information (PHI) and Electronic Protected Health Information (*ePHI*).

During the course of my employment with **Organization**, I may create, see, hear, or touch Protected Health Information (PHI), electronic Protected Health Information (*ePHI*), and other information that **Organization** must maintain as confidential.

By reading and understanding this *Confidentiality* Agreement, I acknowledge and understand that:

- I will not use or disclose PHI or *ePHI*, except when necessary to perform my job.
- With respect to other types of confidential information, I will only *Access*, use, or disclose such information if it is required for the performance of my job.
- I will keep all security codes and *password*s used to *Access* the *facility*, equipment or computer systems, confidential at all times.
- When my employment with **Organization** is terminated or completed, I will immediately return all property to **Organization**. This property includes, but is not limited to, keys, *Access* cards, **Organization** documents however stored or maintained, and ID badges.
- Even after my employment is concluded, I agree to meet the use, disclosure, and *confidentiality* obligations under this *Confidentiality* Agreement.

By reading and understanding this *Confidentiality* Agreement, I am confirming that I am bound by its terms, and that I will perform my duties in accordance with those terms. I understand that if I violate or fail to follow the terms of this *Confidentiality* Agreement, I am subject to disciplinary action, including (but not limited to) termination of my employment and may be subject to civil or criminal penalties.

Introduction to the HIPAA Security Manual

It is the intent of this Policy Manual, along with our other Policy manuals and stand-alone policies, to reflect **Organization**'s responsibilities in ensuring the *confidentiality*, privacy, and security of individual health information that we use, transmit, create, and receive. This Policy Manual, along with our other Policy manuals and stand-alone policies, outlines the responsibilities we have in ensuring that protected health information (PHI) in electronic form, known as electronic protected health information (*ePHI*), is securely used, disclosed, created, maintained, and transmitted by us.

This Policy Manual also addresses our responsibilities to train our workforce so that the workforce is aware of how *ePHI* may and may not be not be viewed or transmitted, and so the workforce is aware of what measures it must take to protect that *ePHI*, in terms of *administrative safeguards* (e.g., following this policy, responding to and reporting *security incidents*), keeping it physically secure, and keeping it technically secure.

Your understanding of the protections we use to keep *ePHI* secure, when and how individuals can *Access* this information, and what to do when you notice it may have been used improperly, are all integral parts of your work duties whenever you work with *ePHI* on **Organization**'s behalf.

As a workforce member of **Organization**, you are responsible for following the safeguards we use to ensure the privacy, *integrity* and security of *ePHI*. You are also responsible for not using or sharing *ePHI* when it is not required for you to perform your job responsibilities.

You are responsible for reading and understanding the Synopses of all the Policies included in this manual, as well as the full content of any policies that apply directly to your role. Organization appreciates your efforts and contributions in meeting the requirements that apply to individuals' protected health information that has been entrusted to us.

The Policies in this Manual have been organized in a way to help you understand the general rules associated with keeping *ePHI* secure. These rules cover how to determine risk to *ePHI*, how to remediate that risk, who to contact with questions about your role and responsibility with respect to *ePHI*, when it is appropriate for you to *Access ePHI* and on what devices such *Access* is appropriate. Please note that while this Security Manual addresses *ePHI* in particular, PHI *in all forms*, including non-electronic protected health information, must be safeguarded. The Privacy Manual should be consulted for policies on safeguarding of PHI.

The rules in this Security Manual also cover what training we provide you with respect to security concepts such as *passwords*, *malicious software*, how to properly *Access ePHI*; how

to respond to incidents where the security of *ePHI* may have been jeopardized; how to prepare for emergency situations that may damage *ePHI*; and how to keep *ePHI* physically safe (e.g., by backing up data, *Access*ing *ePHI* only when, where, and how you have been authorized to do so,) and technically secure (by being familiar with security principles that include automatic logoff, *Access* controls, verification and authorization of identity, *ePHI integrity*, and *encryption*).

Additionally, the Manual covers how **Organization** responds to instances of failing to follow its terms, by applying appropriate disciplinary measures. The table of contents, synopses or any search feature on your browser should help you in finding information to address most situations regarding the security of *ePHI* that you may encounter. Always contact the Security Official or your supervisor for assistance when you are unsure how to proceed.

Security Manual Synopsis

This section is for all workforce members to review and attest. Below is a summary of each policy, including the relevant HIPAA regulations.

If a particular policy applies to your role or position, you must read the entire policy, not just the synopsis.

To view the full policy of a section, please click on the title of that section in the synopsis.

Definitions for the terms used in this Security Manual are included in the Glossary at the end of the manual.

Security Policy 1.0 Security Rule Basics

The HIPAA Security Rule contains measures to protect the *confidentiality*, *integrity*, and *availability* of protected health information that is stored in electronic form. This PHI is referred to as electronic protected health information, or *ePHI* for short.

1. ***Confidentiality*** ensures that no unauthorized *Access* or disclosure is made to *ePHI*;
2. ***Integrity*** ensures that no unauthorized modifications, additions, or deletions are made to *ePHI*; and
3. ***Availability*** ensures that *ePHI* is *Access*ible when needed, and that it is in usable form.

The objective of Security Rule compliance is to protect against and mitigate *security incidents*. To comply with the Security Rule, this **Organization**, a covered entity under HIPAA, has developed and implemented various security processes, policies, and procedures. These are set forth in this manual, the Security Rule self-audits, and other documentation.

What are the Basic Requirements of the Security Rule?

Under the Security Rule, **Organization** will meet the following requirements, with measures appropriate to its size and operations:

1. Ensure the *confidentiality*, *integrity*, and *availability* of all electronic protected health information **Organization** creates, receives, maintains, or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security or *integrity* of such information.
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Rule.
4. Ensure compliance with this subpart by its workforce.

How Does the Security Rule Work?

The Security Rule includes administrative, physical, and *technical safeguards*, and **Organization**al requirements. These safeguards and requirements comprise standards to protect the *confidentiality*, *integrity*, and *availability* of *ePHI*.

Administrative safeguards consist of administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of *security measures* to protect electronically protected health information. These safeguards also

serve to manage the conduct of **Organization**'s workforce to ensure the workforce protects that information.

Physical safeguards protect the physical security of **Organization**'s facilities and devices where *ePHI* may be maintained or *Access*ed.

Technical safeguards are a series of technical measures, such as firewalls, *encryption*, audit controls, and *Access* controls, designed to preserve the *confidentiality*, *integrity*, and *availability* of *ePHI*.

Assigned Security Responsibility:
Organization has an official who has final responsibility for our security. This individual is the HIPAA Security Official.

The HIPAA Security Official is responsible for ensuring that **Organization** develops and implements HIPAA Security Rule policies and procedures, and that each department follows these policies and procedures.

The Security Official monitors, audits, reviews, and enforces **Organization**'s compliance with these policies, and with the HIPAA Security Rule. In addition, the Security Official creates and maintains a mechanism for workforce members to report incidents and suspected HIPAA Security Rule violations.

The Security Official serves as a security point of contact for **Organization**. The Security Official is authorized to speak on **Organization**'s behalf with respect to security-related matters.

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*

Security Policy 2.0 Security Management Process

Organization has a security management process. This process consists of four components:

1. Risk Analysis
2. Risk Management
3. Sanctions
4. *Information systems* Activity and Review

Risk Analysis:

Organization conducts at least an annual risk analysis. The purpose of the risk analysis is to:

1. Determine if security controls are correctly implemented, and, as implemented, are effective in their application;
2. Ensure that HIPAA security regulations, policies, and directives are complied with; and
3. Implement *security measures* sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level for **Organization's** size and operations.

The risk analysis consists of six steps:

1. Collecting data to determine where *ePHI* is stored.
2. Identifying and Documenting Potential Threats and Vulnerabilities to *ePHI*.
3. Assessing Current *Security measures*.
4. Determining the Likelihood of Threat Occurrence.
5. Determining the Potential Impact of Threat Occurrence to *ePHI*
6. Determining the Level of Risk to *ePHI*.

Additional risk analyses will be conducted when:

1. New technology is implemented that either contains *ePHI*, or is used to protect *ePHI*.
2. New facilities that maintain or house *ePHI* are created or established.
3. Existing facilities that maintain or house *ePHI* are being remodeled or the design layout is being altered.
4. New programs, functions, or departments that affect the security of **Organization** are added.
5. Security breaches are identified.
6. There has been a change to HIPAA regulations or other relevant law.
7. There has been a change in personnel with administrative privilege *Access* to critical systems containing *ePHI*.

Once the initial risk analysis has been completed, **Organization** will perform risk management. Risk management consists of implementing *security measures* sufficient to reduce risks and vulnerabilities found in the risk analysis to a reasonable and appropriate level.

Organization will ensure that the workforce complies with **Organization**'s policies and procedures, through a formal disciplinary program that provides for discipline of workforce members found to have violated established security policies and procedures.

Organization will perform *information system* activity review. **Organization** will regularly review records of *information system* activity, such as audit logs, *Access* reports, and

security incident tracking reports. Such review is necessary to ensure that the *confidentiality*, *integrity*, and *availability* of *ePHI* is maintained.

§164.308(a)(1)(ii)(A) *Risk analysis*
§164.308(a)(1)(ii)(B) *Risk management*
§164.308(a)(1)(ii)(C) *Sanctions Policy*
§164.308(a)(1)(ii)(D) *Information system Activity Review*

Security Policy 3.0 Workforce Security

Organization will document the names, job roles and levels of *Access* to *ePHI* of all workforce members. To ensure that members of the workforce have appropriate *Access* to *ePHI* at all times, **Organization** will utilize workforce *security measures*.

Workforce Security consists of three components:

1. **Authorization and Supervision. Organization** requires the authorization of workforce members who work with *ePHI*. **Organization** has procedures that determine which individuals are authorized to work with *ePHI*, in accordance with a role-based approach. **Organization** determines who is responsible for supervising workforce members who work with *ePHI*, or who work in locations where it might be *Access*ed.
2. **Workforce Clearance Procedure. Organization** has procedures to determine that a workforce member's *Access* to *ePHI* is appropriate. These procedures provide for review of role definitions and assignments for appropriateness, at least annually.
3. **Termination Procedure. Organization** has procedures to terminate *Access* to *ePHI* when the employment of, or other arrangement with, a workforce member ends, or when **Organization** determines that it is not appropriate for a certain workforce member to have *Access* to *ePHI*. These procedures will provide for the following measures (among others):

    - Physical *security measures*, if any, including retrieving keys and *Access* cards, and changing locks;
    - Deactivation of computers and other electronic tools;
    - Deactivation of *Access* accounts;
    - Disabling of *user*s and *password*s; and
    - Completion of an employee termination checklist.

§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*

Security Policy 4.0 Information *Access* Management

Organization has an information *Access* policy that contains procedures for authorizing *Access* to *ePHI*. These procedures for authorizing *Access* to *ePHI* are consistent with the requirements of the HIPAA Privacy Rule. These procedures serve to limit unauthorized *Access* to, use of, and disclosure of *ePHI*. The information *Access* policy provides guidelines on how workforce *Access* to *ePHI* is granted. The information *Access* policy contains procedures for:

- ***Access* Authorization. Organization** has policies and procedures providing for a formal system for authorizing *user Access* to *ePHI*, for example, through *Access* to a *workstation*, transaction, program, or process. **Organization**'s procedures for granting *Access* to *ePHI* use a role-based approach. See this Security Manual for details.
- ***Access* Establishment and Modification. Organization** has procedures that, based upon its *Access* authorization policies, establish, document, review, and modify a *user*'s right of *Access* to *ePHI*. These procedures are governed by the principle of "least privilege," which means that *user*s must be able to *Access* only that *ePHI* that is necessary to perform their job functions. **Organization** will regularly review *Access* and *Access* levels to ensure that these are appropriate. **Organization** requires prompt initiation of account termination or modification when appropriate.

§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*

Security Policy 5.0 Security Awareness and Training

All members of **Organization's** workforce will receive security training. **Organization** will require *user*s to complete security training and attestation in The Guard at least on hire, and annually for all employees. **Organization** will document all attestations. Attestations are employees' written acknowledgments that they understand **Organization**'s security policies and procedures and agree to abide by them.

Security Awareness and Training consists of the following:

- **Security reminders**, which **Organization** will provide in the form of periodic security updates.
- **Training on protection from *malicious software*. Organization** uses a variety of measures to guard against, detect, and report *malicious software*.
- **Training on login monitoring.** Login monitoring consists of procedures for monitoring log-in attempts and reporting discrepancies.
- **Training on *password* management.** *Password* management consists of procedures for creating, changing, and safeguarding *password*s.

Security Reminders:
Security reminders, in the form of periodic security updates, will be provided to workforce members as appropriate.

Protection from *Malicious software*:
Organization has policies and procedures for guarding against, detecting, and reporting *malicious software*, and will train employees on these policies and procedures. Examples of security controls include:

- Endpoint protection (AV/Antimalware, etc.);
- *Encryption* of data in transit and at rest;
- Procedures for reporting and addressing *security incidents* and breaches;
- Installation of operating system and third party application updates (patches);
- Changing or removing default logins and *password*s on routers, firewalls, network switches, wireless *Access* points, Internet of Things (IOT) devices, and *Access* control systems;
- Disabling of unnecessary software and applications on systems storing *ePHI*;
- Periodic installation and updating of malware protection software;
- Setting of proper file/directory/ownership/permissions;
- Regularly reviewing HIPAA *workstation* browser settings;
- Regularly reviewing email client settings;
- Performing periodic network and system vulnerability scans and correcting discovered vulnerabilities;
- Implementing email malicious code filtering;
- Installing and enabling firewalls; and
- Installing intrusion detection software and/or systems to detect the threat of unauthorized remote *Access*.

Login Monitoring:
Organization requires *user Access* logging for all systems (hardware or software) with *Access* to *ePHI*. For all systems that contain *ePHI*, **Organization** will review *user Access* logs periodically as part of a risk analysis or as otherwise required by the HIPAA Security Rule. **Organization** trains the workforce on what *user Access* logging is, and how it is performed.

***Password* Management:**
Organization has implemented procedures for creating, changing, and safeguarding strong *password*s. All workforce members will use strong *password*s to *Access workstation*s. **Organization** trains all workforce members on how to create, change, and safeguard these *password*s.

Organization's strong *password* policy follows National Institute of Standards and Technology (NIST) guidance, and requires:

- A minimum of eight characters and a maximum length of at least 64 characters.
- The ability to use all special characters but no special requirement to use them.
- Restriction of sequential and repetitive characters (e.g. 12345 or aaaaaa).
- Restriction of context specific *password*s (e.g. the name of the site, etc.).
- Restriction of commonly used *password*s (e.g. p@ssw0rd, etc.) and dictionary words.
- Restriction of *password*s obtained from previous breach incidents.

Organization prohibits the sharing of *password*s. Workforce members may not share *password*s with other employees, managers, visitors, family members, friends, or anyone else. Workforce members will use a *password* management solution. This means workforce members will either:

- Commit *password*s to memory, or,
- Store *password*s in an **Organization**-approved credentials management system.

§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*

Security Policy 6.0 Incident Response and Reporting

A security incident is the attempted or successful unauthorized *Access*, use, disclosure, modification, or destruction of information or interference with system operations in an *information system*.

Organization has procedures to address *security incidents*. Through these procedures, **Organization**:

- Identifies and responds to suspected or known *security incidents*;
- Mitigates, to the extent practicable, the harmful effects of *security incidents* that are known to **Organization**; and
- Documents *security incidents* and their outcomes.

In addition to this policy, please also refer to *Security Policy 20.0* and *Security Policy 21.0.* The policies provide additional information related to *security incidents* and to breaches of unsecured PHI.

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

Security Policy 7.0 Contingency Plan

Organization, to be prepared for emergencies and to ensure smooth recovery from emergencies, uses a series of contingency plans. **Organization** evaluates, tests, and updates contingency plans, as needed. Contingency plans include:

- **A data backup plan.** In the data backup plan, **Organization** utilizes measures to create and maintain retrievable exact copies of electronic protected health information.
- **A disaster recovery plan.** In the disaster recovery plan, **Organization** utilizes a series of measures to restore any loss of data.
- **An emergency mode operation plan, also known as a Business Continuity Plan (BCP).** The Business Continuity Plan contains procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while **Organization** operates in emergency mode.

Organization's data backup plan, disaster recovery plan, and business continuity plan, contain testing and revision procedures. Through testing, **Organization** will determine whether plans are working and what periodic updates are needed. **Organization** will also periodically perform an applications and data criticality analysis. This is an assessment of the relative criticality of specific applications and data in support of the other plan components. This assessment will allow **Organization** to determine which applications and data require priority attention in the event of an emergency.

§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*

Security Policy 8.0 Monitoring and Effectiveness

Organization will periodically perform a technical and nontechnical evaluation of its security policies and procedures. **Organization** will perform these evaluations in response to environmental or operational change affecting the security of *ePHI*. The evaluation will establish the extent to which **Organization**'s security policies and procedures meet the requirements of the Security Rule. **Organization** will identify who determines when evaluation is necessary; how updates based on evaluations are to be made; and ensure that all evaluations and changes to policies and procedures are appropriately documented and/or disseminated.

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

Security Policy 9.0 Business Associate Relationships

Organization, as a covered entity, may enter into business relationships with vendors. If these relationships require the vendor to *Access ePHI*, the relationship will be formalized in a legally binding contract called a business associate agreement, under which the vendor is a business associate. The contract requires each party to undertake specific actions to ensure the *confidentiality*, *integrity*, and *availability* of PHI. **Organization** will investigate and act on complaints it receives about business associates. For additional information on business associates, see Privacy Policy 9.0, *Business Associates*.

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

Security Policy 10.0 *Facility Access* Controls

Organization utilizes *facility Access* controls. These controls are a series of measures to reasonably safeguard *ePHI* and equipment stored in a physical location.

Organization's *facility Access* controls include:

- Procedures to limit physical *Access* to electronic *information system*s and the facilities in which they are housed, while ensuring that properly authorized *Access* is allowed.
- Procedures for *facility Access* in support of restoration of lost data under **Organization**'s disaster recovery plan and business continuity plan in the event of an emergency.
- Policies and procedures to safeguard the *facility* and its equipment from unauthorized physical *Access*, tampering, and theft.
- Procedures to control and validate a person's *Access* to facilities based on their role or function, including visitor control and control of *Access* to software programs for testing and revision.
- Policies and procedures to document repairs and modifications to the physical components of a *facility* that are related to security (for example, hardware, walls, doors, and locks).

§164.310(a)(1) *Facility Access controls*
§164.310(a)(2)(i) *Contingency operations*
§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*

Security Policy 11.0 *Workstation* Use and *Workstation* Security

Organization utilizes *workstation Access* controls. These *Access* controls, which ensure access is appropriate and authorized, are for computing devices as well as electronic media that store *ePHI*.

For computing devices, **Organization** utilizes *workstation Access* controls to adequately protect all observable *ePHI* from unauthorized disclosure or *Access* on computer screens. **Organization** requires the workforce to ensure that *ePHI* and other confidential information on computer screens is not visible to unauthorized persons. **Organization** also utilizes *workstation Access* controls for workforce members who use laptops and other portable computing devices while telecommuting or traveling.

Organization utilizes controls for electronic media that store PHI. These media include hard drives, flash drives, USB drives, as well as other portable media on which *ePHI* is stored.

Organization requires workforce members to protect *ePHI* on all computing devices and on all electronic media, regardless of where the device or media is used or located.

§164.310(b) *Workstation use*
§164.310(c) *Workstation security*

Security Policy 12.0 Device and Media Controls

Organization utilizes procedures governing the receipt and removal of hardware and electronic media that contain *ePHI* in and out of a *facility*, and the movement of these items within the *facility*.

These procedures cover:

- ***ePHI Disposal.*** **Organization** requires proper final disposal of *ePHI* and/or the hardware or electronic media on which it is stored.
- ***Media re-use controls.*** **Organization** uses a series of controls for removal of electronic protected health information from electronic media before the media are made available for reuse.
- ***Accountability controls.*** **Organization** maintains a record of the movements of hardware and electronic media, and any person responsible for such movement.
- ***Data Backup and Storage.*** **Organization** creates a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

§ 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*

Security Policy 13.0 *Access* Controls

Organization safeguards the *confidentiality*, *integrity*, and *availability* of electronic protected health information. To do this, **Organization** manages who can *Access ePHI*, implementing ***user Access*** measures.

Organization employs following *user Access* measures:

- Assignment of a unique name and/or number for identifying and tracking *user* identity.
- Measures for obtaining necessary electronic protected health information during an emergency.
- Electronic procedures that terminate an electronic season after a predetermined time of inactivity.
- A mechanism to encrypt and decrypt electronic protected health information.

§164.312(a)(1) *Access control*

Security Policy 14.0 Audit Controls

Organization utilizes mechanisms to record and examine *information system*s activity on hardware and software. These mechanisms are known as audit logs. **Organization** utilizes mechanisms for audit log creation, examination of the activity in audit logs, and for log retention. **Organization** reviews audit logs for unauthorized activity.

§164.312(b) *Audit controls*

Security Policy 15.0 *Integrity* Controls

Organization protects electronic protected health information from improper alteration or destruction. To do this, **Organization** maintains audit and *Access* logs for electronic health record content. **Organization** also uses electronic mechanisms that corroborate that *ePHI* has not been destroyed in an unauthorized manner. These mechanisms determine whether *ePHI* has been altered or destroyed, and, if so, whether the alteration or destruction is unauthorized.

45 CFR 164.312(c) *Integrity*

Security Policy 16.0 Person or Entity *Authentication*

Organization verifies that a person or entity seeking *Access* to electronic protected health information, is in fact the person or entity he, she, or it claims to be. Person or entity *authentication* measures include:

- Proper configuration of systems and applications, so that they do not save *password*s.
- Providing *user*s with unique *user*names and *password*s.
- Strong *password*s.

- Periodic review for *workstation*, operating system, and application logs, as well as failed or successful changes to account permissions.
- Two-factor *authentication* (2FA) and multi-factor *authentication* (MFA).
- Biometric *Access* or biometric identifiers.

164.312(d) *Person or Entity Authentication*

Security Policy 17.0 Transmission Security

Organization has *security measures* to guard against unauthorized *Access* to *ePHI* being transmitted over an electronic communications network. Through these measures, **Organization** ensures that electronically transmitted *ePHI* is not improperly modified without detection until disposed of. **Organization**, to maintain transmission security, encrypts electronic protected health information whenever deemed appropriate.

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

Security Policy 18.0 ePHI Safeguards

This policy addresses the safeguarding of *ePHI* received, created, used, maintained, and/or transmitted through various electronic media. **Organization** will safeguard *ePHI* unauthorized *Access* during the communication process. **Organization** requires that *ePHI* is only disclosed to personnel, patients, their personal representatives, other covered entities, public health officials, and business associates, in accordance with HIPAA regulations and this policy.

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*

Security Policy 19.0 Policies and Procedures

Organization develops and implements HIPAA Security Rule policies and procedures, as necessary. **Organization** will revise these when changes in regulations or changes in the work environment take place. Organization will regularly review these procedures and document the reviews. **Organization** will maintain documentation of all policies, procedures, and other writings, as required under the Security Rule.

§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*

Security Policy 20.0 HIPAA Incident Response and Reporting and Breach Determination

Organization will identify and respond to suspected incidents, require its *workforce members* to report incidents, and determine when there is a reportable *breach* of an *individual*'s *PHI*.

Organization uses a *Breach* Determination Policy to meet **Organization's** responsibilities and to provide guidance to **Organization** *workforce members* on how to recognize and report a privacy or *security incident* involving electronic protected health information. **Organization** follows the procedures set in Security Policy 20.0 forth to determine if there has been a *Breach* (an acquisition, *Access*, use, or disclosure of the Member's *unsecured PHI* in a manner not permitted under *HIPAA.* Unsecured PHI includes both "paper" PHI as well as ePHI).

This policy establishes guidelines for **Organization** to:

- Require the reporting of suspected privacy and *security incidents* (any attempted or successful unpermitted or unauthorized *Access*, use, disclosure, modification, interference or destruction of *unsecured PHI* in any form). All *workforce members* are required to report any suspected incident to the Compliance, Privacy or Security Official as soon as possible, and may report anonymously through The Guard if preferred. Failure to promptly report any suspected or known incident will result in disciplinary action.
- Identify and respond to suspected or known incidents involving the security or privacy of protected health information, including mitigating any harmful effects. Any complaint that is filed with the **Organization** that is potentially a privacy or *security incident* will be handled under this Policy, which also appears in the Security manual, instead of Privacy Policy 5.0: *Complaints to the* ***Organization***.
- Determine if there has been a *Breach* of *unsecured PHI* ("*PHI*") after analyzing potential exceptions and performing a risk analysis, and
- Document the incidents, responses and *Breach* determinations.
- Follow the *Breach* Notification Policy whenever it determines that a *Breach* has occurred. See Privacy Policy 7: *Breach Notification*.

45 CFR 164.308(a)(6)(i) *Security Incident Procedures*
45 CFR 164.308(a)(6)(ii) *Implementation Specification: Response and Reporting (Required)*
45 CFR 164.530(a)(c)(e)(f) *Administrative Requirements: Personnel Designations, Safeguards, Sanctions and Documentation, Mitigation*
45 CFR 164.402 *Definitions: Breach*

Security Policy 21.0 Breach Notification

Organization will determine when there is a reportable *breach* of an *individual*'s *PHI,* and will make appropriate and timely notifications following a *breach*.

Organization uses this breach notification policy to set forth *workforce member* responsibilities and to provide guidance to *workforce members* regarding making required notifications when a *Breach* determination has been made under Privacy Policy 6.0: *Incident Response and Reporting and Breach Determination*.

This *Breach* Notification Policy establishes guidelines for **Organization** to:

- Make, or ensure the appropriate *Covered entity* or *Business associate* makes, appropriate notifications to *individual*s impacted by a *Breach*;
- Make, or ensure the appropriate *Covered entity* or *Business associate* makes, appropriate notifications to federal and state authorities if required by the details of the *Breach* determination;
- Make, or ensure the appropriate *Covered entity* or *Business associate* makes, appropriate notifications to media if the findings of the *Breach* determination require them;
- Determine when and if appropriate substitute notice is allowed and to use that substitute notice when appropriate; and
- Document compliance with the requirements of *Breach* notifications.

45 CFR 164.404 *Notification to Individuals*
45 CFR 164.406 *Notification to the Media*
45 CFR 164.408 *Notification to the Secretary*
45 CFR 164.410 *Notification by a Business Associate*
45 CFR 164.412 *Law Enforcement Delay*
45 CFR 164.414 *Administrative Requirements and Burden of Proof*
45 CFR 164.530 *Administrative Requirements*

Attestation

I hereby attest and acknowledge that I have read and understood the contents of this *HIPAA* Security Policy and Procedure Manual. Through my attestation, I hereby confirm that I am bound by **Organization's** security policies and procedures and will perform my job duties accordingly. I understand that if I violate any **Organization** security policy or procedure, I am subject to disciplinary action, up to and including termination of my employment. I may also be subject to civil or criminal penalties.

I hereby acknowledge and agree that this attestation is the equivalent of a physical or e-signature.

Security Policy 1.0 Security Rule Basics

FULL POLICY LANGUAGE

Policy Purpose:

To inform the workforce of the basic requirements of the HIPAA Security Rule.

Policy Description:

The HIPAA Security Rule consists of measures to protect the *confidentiality*, *integrity*, and *availability* of electronic protected health information (*ePHI*). Electronic protected health information, or *ePHI*, is protected health information stored in electronic form. The Security Rule requires that **Organization** take a series of administrative, physical, and technical measures to protect the *confidentiality*, *integrity*, and *availability* of electronic protected health information.

- ***Confidentiality* measures** ensure that no unauthorized *Access* is made to *ePHI*, and that there is no unauthorized disclosure of *ePHI*;
- ***Integrity* measures** ensure that no unauthorized modifications are made to *ePHI*; and
- ***Availability*** measures ensure that *ePHI* is *Access*ible when needed, and that it is in usable form.

The objective of Security Rule compliance is to protect against and mitigate *security incidents*. To comply with the Security Rule, **Organization** has developed and implemented various security processes, policies, and procedures, which are set forth in this manual.

What are the Basic Requirements of the Security Rule?

Under the Security Rule, **Organization** must do the following:

- Ensure the *confidentiality*, *integrity*, and *availability* of all electronic protected health information **Organization** creates, receives, maintains, or transmits.

- Protect against any reasonably anticipated threats or hazards to the security or *integrity* of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Rule.
- Ensure compliance with the Security Rule by its workforce.

How Does the Security Rule Work?
The Security Rule includes administrative, physical, and *technical safeguards*, and organizational requirements. These safeguards and requirements set forth rules to protect the *confidentiality*, *integrity*, and *availability* of *ePHI*.

What are Safeguards?
The Security Rule requires implementation of three types of safeguards: 1) administrative, 2) physical, and 3) technical. Each safeguard contains standards that specify how the standard is to be implemented. Each standard contains implementation specifications.

What are *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).

The security management process standard, 45 CFR 164.308(a)(1), requires **Organization** to implement policies and procedures to prevent, detect, contain, and address security violations.

To implement the standard, **Organization** will perform a security risk analysis, conduct risk management, apply appropriate sanctions against workforce members who fail to comply with **Organization**'s security policies and procedures, and conduct *information system* activity review. *Information system* activity review includes regular review of records of *information system* activity, such as audit logs, *Access* reports, and security incident tracking reports.

The remaining *administrative safeguards* are as follows:

1. Designation of a security official, who is responsible for the development and implementation of our Security Rule policies and procedures. (45 CFR 164.308(a)(2)).
2. Implementing workforce *security measures* to:
    a. Ensure that all members of the workforce have appropriate *Access* to electronic protected health information; and

   b. Prevent those workforce members who are not given *Access* to *ePHI*, from obtaining such *Access*. (45 CFR 164.308(a)(3)).
2. Implementing policies and procedures for authorizing *Access* to electronic protected health information. (45 CFR 164.308(a)(4)).
3. Implementing a security awareness and training program for all workforce members, including management. (45 CFR 164.308(a)(5)).
4. Implementing policies and procedures to address *security incidents*. (45 CFR 164.308(a)(6)).
5. Establishing (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain *ePHI*. (45 CFR 164.308(a)(7)).
6. Performing a periodic technical and nontechnical evaluation that establishes the extent to which our security policies and procedures meet the requirements of the Security Rule. (45 CFR 164.308(a)(8)).

45 CFR 164.308(b) provides that we, as a covered entity, may permit a business associate to handle our *ePHI*, but only if we and the business associate agree, through a written business associate agreement or contract that the business associate will appropriately safeguard the information.

What Are *Physical safeguards*?
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; and
- Locking of areas where *ePHI* is stored.

Physical safeguard control and *security measures* include:

- ***Facility Access* and Control Measures. Organization** limits physical *Access* to facilities, while allowing authorized *Access* to *ePHI* (164.310(a)(1)). *Facility Access* and control measures include:
  - ***Contingency operations.* Organization** utilizes measures to ensure *facility Access* in support of restoration of lost data (164.310(a)(2)(i)).
  - ***Facility security plan.*** Here, **Organization** uses measures to safeguard the *facility* and the equipment therein from unauthorized physical *Access*, tampering, and theft (164.310(a)(2)(ii)).
  - ***Access control and validation procedures.*** Here, **Organization** uses measures to control and validate a person's *Access* to facilities based on their role or function, including visitor control, and control of *Access* to software programs for testing and revision (164.310(a)(2)(iii)).

    - ***Maintenance records.*** Here, **Organization** takes steps to document repairs and modifications to the physical components of a *facility* that are related to security (164.310(a)(2)(iv)).
- ***Workstation* Use Measures**. **Organization** ensures that *workstation*s are properly *Access*ed and used (164.310(b)).
- ***Workstation Security measures*: Organization** ensures that *Access* to *workstation*s is restricted to authorized *user*s (164.310(c)).
- **Device and Medial Controls. Organization** utilizes measures to govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a *facility*, and the movement of these items within the *facility* (164.310(d)(1)). To do this, **Organization:**
    - Uses ***disposal measures*** (164.310(d)(2)(i)). These address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
    - Utilizes ***media re-use measures*** (164.310(d)(2)(ii)). These measures provide for removal of electronic protected health information from electronic media before the media are made available for reuse.
    - Takes ***accountability measures*** (164.310(d)(2)(iii)). Here, **Organization** maintains a record of the movements of hardware and electronic media and any person responsible for these media.
    - Utilizes ***data backup and storage measures*** (164.310(d)(2)(iv)). **Organization** creates a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

What are *Technical safeguards*?
Technical safeguards include measures, such as endpoint protection, firewalls, *encryption*, and data backup, that ensure that *ePHI* is properly *Access*ed, monitored, and maintained. These safeguards consist of the following:

- ***Access* Controls.** Here, **Organization** uses technical measures to ensure that only authorized persons can *Access ePHI* (164.312(a)(1)). *Access* controls measures include:
    - ***Unique user identification.*** Here, **Organization** assigns a unique name and/or number for identifying and tracking *user* identity (164.312(a)(2)(i)).
    - ***Emergency Access procedure.*** Here, **Organization** utilizes a series of measures to obtain necessary electronic protected health information during an emergency (164.312(a)(2)(ii)).
    - ***Automatic logoff.*** Here, **Organization** utilizes electronic procedures that terminate an electronic session after a predetermined time of inactivity (164.312(a)(2)(iii)).
    - ***Encryption and decryption.*** Here, **Organization** utilizes a mechanism to encrypt and decrypt electronic protected health information at rest and in transit (164.312(a)(2)(iv)).

- **Audit Controls.** Here, **Organization** utilizes hardware, software, and/or procedural mechanisms to *record and examine Access* in *information systems* that *contain or use ePHI* (164.312(b)).
- ***Integrity* Controls.** Here, **Organization** takes measures to protect electronic protected health information from improper alteration or destruction. (164.312(c)(1)). These measures serve to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. (164.312(c)(2)).
- **Person or entity *authentication.*** Here, **Organization** utilizes measures to verify that a person or entity seeking *Access* to electronic protected health information is the one claimed (164.312(d)).
- **Transmission Security.** Transmission *security measures* guard against unauthorized *Access* to *ePHI* that is transmitted over an electronic network (164.312(e)). Transmission *security measures* include:
    - ***Integrity* controls**. Here, **Organization** must implement *security measures* to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until it is disposed of (164.312(e)(2)(i)).
    - ***Encryption*.** Here, **Organization** must implement a mechanism to encrypt electronic protected health information whenever it has been deemed appropriate to do so (164.312(e)(2)(ii)).

Required vs. Addressable Standards:
Some Security Rule standards include required or addressable implementation specifications. For example, the Technical Safeguard's *access control* standard contains four implementation specifications. These are unique *user* identification, emergency *Access* procedure, automatic logoff, and *encryption* and decryption. Unique *user* identification and emergency *Access* procedure are "required," while automatic logoff and *encryption* and decryption are "addressable."

When an implementation specification is required, **Organization** will implement the specification. When we decide which *security measures* to use, we will take into account:

- Our size, complexity, and capabilities.
- Our technical infrastructure, hardware, and software security capabilities.
- The costs of *security measures*.
- The probability and criticality of potential risks to electronic protected health information.

When an implementation specification is addressable, we will:

- Assess whether each implementation specification is a reasonable and appropriate safeguard in our environment, when analyzed with reference to the likely contribution to protecting electronic protected health information.
- Implement the specification if it is reasonable and appropriate to do so.

If implementing the implementation specification is not reasonable and appropriate, we will document why it would not be reasonable and appropriate to implement the implementation specification, and will implement an equivalent alternative measure if reasonable and appropriate.

The HIPAA Security Rule protects the *confidentiality*, *integrity*, and *availability* of protected health information that is stored in electronic form. This PHI is referred to as electronic protected health information, or *ePHI* for short.

- ***Confidentiality*** ensures that no unauthorized *Access* or disclosures are made to *ePHI*;
- ***Integrity*** ensures that no unauthorized modifications are made to *ePHI*; and
- ***Availability*** ensures that *ePHI* is *Access*ible when needed, and that it is in usable form.

The objective of Security Rule compliance is to protect against and mitigate *security incidents*. To comply with the Security Rule, this **Organization** has developed and implemented various security processes, policies, and procedures. These are set forth in this manual, the Security Rule self-audits, and other documentation.

Assigned Security Responsibility:

Organization will have one, and only one, individual that is assigned to HIPAA security responsibility (the "HIPAA Security Official"). This individual should be a senior-level individual.

The HIPAA Security Official is responsible for developing and implementing **Organization's** security policies and procedures, and that each department follows these policies and procedures.

These policies and procedures, which are set forth in this manual, must be reviewed and approved by the Security Official before they are disseminated to staff. Once the Security Official reviews the policies and procedures, and any updates to policies and procedures, **Organization** must disseminate the policies and procedures to staff.

The Security Official monitors, audits, reviews, and enforces **Organization**'s compliance with these policies, and with the HIPAA Security Rule. In addition, the Security Official creates and maintains a mechanism for workforce members to report incidents and suspected HIPAA Security Rule violations.

The Security Official ensures that all documentation required to be maintained by the Security Rule is maintained for the appropriate length of time.

The Security Official serves as a security point of contact for **Organization**. The Security Official is authorized to speak on **Organization**'s behalf with respect to security-related matters.

Organization will document the designation of the Security Official.

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*

Security Policy 2.0 Security Management Process

FULL POLICY LANGUAGE

Policy Purpose:

Organization utilizes security management process measures to prevent, detect, contain, and address security violations. This policy sets forth these measures, which include risk analysis, risk management, a workforce sanctions policy, *information systems* activity review, and a corrective action plan.

Policy Description:

Organization utilizes a series of measures to prevent, detect, contain, and correct security violations. These measures are part of **Organization**'s security management process. The measures include:

- Completion of a periodic security risk analysis (SRA). This analysis reveals what mitigation measures, if any, are appropriate.
- risk management and mitigation based on the results of the security risk analysis.
- Administering disciplinary measures when appropriate. **Organization** follows a disciplinary process when **Organization** concludes that a workforce member has not complied with **Organization**'s established information security policies and procedures.
- Periodic *information system* activity review.
- Development of a corrective action plan, and implementation of that plan when necessary.

Security Risk Analysis Overview:

Organization will begin to analyze security risks by documenting its current *information system* configuration, both inside the firewall and outside of it. **Organization** will maintain copies of this documentation.

Then, **Organization** will periodically assess the potential risk and vulnerabilities to the *confidentiality*, *integrity*, and *availability* of the *ePHI* that it holds. This assessment is known as a security risk analysis. **Organization** will conduct a thorough and accurate security risk analysis (SRA), at least annually. **Organization** will also conduct the analysis upon occurrence of a significant event or change in **Organization**'s operating environment or change in the regulatory landscape.

Events that may require **Organization** to conduct an SRA include (but are not limited to):

- Acquisition or corporate restructuring.
- Hiring or termination of key personnel.
- Addition or subtraction of business associates/vendors with *Access* to *ePHI*.
- Installation or implementation of new technology or tools that interact with or protect *ePHI*.
- New facilities that maintain or house *ePHI* are created or established.
- Existing facilities that maintain or house *ePHI* are being remodeled or the design layout is being altered.
- New programs, functions, or departments that affect the security of **Organization** are added.
- Security breaches are identified.
- Changes in the mode or manner of service delivery are made.
- Changes in the regulatory landscape.

Security Risk Analysis – Concepts:

An SRA is the conducting of an accurate and thorough assessment of the potential risks and vulnerabilities to the *confidentiality*, *integrity*, and *availability* of electronic protected health information held by **Organization**. The following concepts inform how to perform an SRA:

Vulnerability:

A vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

Vulnerabilities, whether accidentally triggered or intentionally exploited, could potentially result in a security incident, such as inappropriate *Access* to or disclosure of *ePHI*.

Vulnerabilities may be grouped into two general categories - technical and non-technical. Non-technical vulnerabilities may include ineffective or non-existent policies, procedures, standards or guidelines. Technical vulnerabilities may include: holes, flaws or weaknesses

in the development of *information system*s; or incorrectly implemented and/or configured *information system*s.

Threat:
A threat is the potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

There are several types of threats that may occur within an *information system* or operating environment. Threats may be grouped into general categories such as natural, human, and environmental.

- Examples of natural threats – threats caused by nature - include floods, earthquakes, tornadoes, and landslides.
- Human threats are enabled or caused by humans, and include both intentional (e.g., network and computer based attacks, *malicious software* upload, and unauthorized *Access* to e-PHI) and unintentional (e.g., inadvertent data entry or deletion and inaccurate data entry) actions.
- Environmental threats come from the physical environment, and include events such as power failures, pollution, chemicals, and liquid leakage.

Risk:
A definition of risk, from NIST SP 800-30, is:
"The net impact, considering (1) the probability that a particular threat will exercise (accidentally trigger or intentionally exploit) a particular vulnerability, and (2) the resulting impact if this should occur . . . . "

Risks are a function of two things:

1. The likelihood of a given threat triggering or exploiting a particular vulnerability; and
2. The resulting impact on **Organization**. This means that risk is not a single factor or event, but rather it is a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on **Organization**.

Scope of the Security Risk Analysis:
Organization's risk analysis will take into account potential risks and vulnerabilities to the *confidentiality*, *availability* and *integrity* of all *ePHI* that **Organization** creates, receives, maintains, or transmits. This includes *ePHI* in all forms of electronic media, such as hard drives and portable electronic devices. Electronic media encompasses something as small as a single *workstation*, all the way through complex networks connected between multiple locations. **Organization**'s risk analysis will therefore take into account all of its *ePHI*, regardless of the particular electronic medium in which it is created, received, maintained or transmitted, or the source or location of its *ePHI*.

Categorization of *Information system*s:
Before performing the risk analysis, **Organization** will document its current *information system* configuration. As **Organization** does this, **Organization** will categorize its *information system*s as high, moderate, or low impact systems. To determine whether an *information system* should be categorized as high, moderate, or low-impact, **Organization** should ask this key question: If the *information system* were unavailable, would the un*availability* have a high, moderate, or low impact on daily operations?

Elements of a Risk Analysis:
A risk analysis consists of six steps. These are listed below.

Step 1: Data Collection:
Organization will identify where *ePHI* is stored, received, maintained or transmitted. **Organization** will identify all devices in your **Organization** that store *ePHI* including removable media, remote *Access* devices, mobile devices, computers, servers, laptops, etc.). **Organization** will also identify where *ePHI* actually *resides*. Does *ePHI* reside in the accounting system, for example? Is it in the Cloud? **Organization** will identify all hardware and software that are used to collect, store, process, or transmit *ePHI*, including excel spreadsheets, word tables, cloud and other like data storage.

Organization will gather relevant data by: reviewing past and/or existing projects; performing interviews; or reviewing documentation. The data on *ePHI* gathered using these methods must be documented.

Step 2: Identify and Document Reasonably Anticipated Threats and Vulnerabilities
Threats:
Organization will identify and document reasonably anticipated threats to *ePHI*. Threats are unique to the circumstances of **Organization's** environment. Examples of threat sources include:

- Natural sources (e.g., floods or earthquakes);
- Human source (e.g., data entry errors or hackers); and
- Environmental sources (e.g., power surges and spikes).

Vulnerabilities:
Organization will identify all vulnerabilities to the *confidentiality*, *integrity*, and *availability* of *ePHI*. Vulnerabilities, whether accidentally triggered or intentionally exploited, may result in a security incident, such as inappropriate *Access* to or disclosure of *ePHI*. To identify vulnerabilities, **Organization** will review and test its Data Backup and Disaster Recovery Plans (described in detail in Security Policy 7.0, *Contingency Plan*), will run vulnerability scans of all systems storing *ePHI*, and will complete the Physical Site Audit.

Step 3: Assess Current *Security measures*:

Organization will assess and document the *security measures* that it uses to safeguard *ePHI*. To perform this assessment, **Organization** will periodically complete the IT Risk Audit, and document all current safeguards.

Step 4: Determine the Likelihood of Threat Occurrence:
Organization will determine the likelihood of threat occurrence. Likelihood determination assesses the possibility of a threat occurring. To determine likelihood, **Organization** will review information from threat and vulnerability identification, and the assessment of existing controls. **Organization** will classify likelihood levels as low, medium and high. A low level of likelihood is where a threat is unlikely to occur. A high level of likelihood is where a potential threat is very likely to occur. **Organization** should perform this likelihood determination assessment in its Disaster Recovery Plan.

The output of the determination assessment is documentation of all threat and vulnerability combinations with associated likelihood estimates that may impact the *confidentiality*, *availability* and *integrity* of **Organization**'s *ePHI*.

Step 5: Determine the Potential Impact of Threat Occurrence:
Organization will determine the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability. To do this, **Organization** will complete the IT Risk Audit, and rank the magnitude of potential impacts, either on a numeric scale (1-10, with one being the lowest impact, and ten being the highest impact), or on a qualitative scale, denoting impacts as "Very High," "High," "Medium," or "Low," as appropriate.

Step 6: Determine the Level of Risk:
Organization will assign risk levels for all threat and vulnerability combinations identified during the previous steps of the risk analysis. The risk level determination should be performed by assigning a risk level based on the average of the likelihood and impact levels you have previously identified. The output of the risk level determination should be documentation of the assigned risk levels and a list of corrective actions to be performed to mitigate each risk level.

Finalize Documentation:
Organization will keep written documentation of the risk analysis when it has been completed, by storing its audits in The Guard.

Risk Management:
Once **Organization** has completed and documented the results of the risk analysis, **Organization** will perform risk management. Risk management, required by the Security Rule, includes the implementation of *security measures* to reduce risk to reasonable and appropriate levels to, among other things, ensure the *confidentiality*, *integrity*, and *availability* of *ePHI*; protect against any reasonably anticipated threats or hazards to the security or *integrity* of *ePHI*, and protect against any reasonably anticipated uses or disclosures of *ePHI* that are not permitted or required under the HIPAA Privacy Rule

As part of risk management, **Organization** will utilize *security measures* sufficient to reduce risks and vulnerabilities, identified in the security risk analysis, to a reasonable and appropriate level. To do this, **Organization** will select, implement, and document appropriate controls to safeguard data, relative to the sensitivity or criticality of that data as determined by the risk analysis. Such controls include, for example, implementing *encryption* at the disc level, installing endpoint protection, and implementing periodic reviews of security controls as part of the IT Risk Audit.

The risk management process consists of three steps:

1. Developing and implementing a risk management plan;
2. Implementing *security measures*; and
3. Evaluating and maintaining *security measures*.

Developing and Implementing a Risk Management Plan:
Developing and implementing the risk management plan provides structure for **Organization**'s evaluation, prioritization, and implementation of risk-reducing *security measures*. The risk management plan will contain implementation measures that address:

- The risks being addressed;
- The *security measures* that **Organization** has selected to reduce the risks; and
- Risk management plan implementation priorities, such as required resources, assigned responsibilities, and start and completion dates.

A completed risk management plan will contain prioritized risks, options for mitigation of those risks, and a plan for implementation. The plan will guide **Organization**'s actual implementation of *security measures* to reduce risks to *ePHI* to reasonable and appropriate levels.

Implementing *Security measures*:
Once **Organization** develops the risk management plan, **Organization** will implement the technical and non-technical measures called for by the plan. **Organization** may choose to use either internal or external resources to complete the activities needed to implement the *security measures*.

Evaluating and Maintaining *Security measures*:
Once **Organization** has implemented risk mitigation measures, it will continue to monitor these measures. To do this, **Organization** will perform risk analysis and risk management in response to changes in its operating environment. The risk analysis will identify new risks or update existing risk levels resulting from environmental or operational changes. The output of the updated risk analysis will be an input to the risk management processes to reduce newly identified or updated risk levels to reasonable and appropriate levels.

Sanctions Policy:

The Security Rule requires **Organization** to apply appropriate sanctions and discipline against workforce members who fail to comply with its security policies and procedures. **Violation of Organization's** security policies or procedures may subject employees to disciplinary action. Depending on the severity of the infraction, disciplinary action may include measures such as retraining, verbal or written warnings, placement on a performance improvement plan, suspension, or termination. **Organization** will make efforts to ensure that disciplinary action that is proposed or taken is as uniform and consistent as possible.

Procedures: Employee Awareness of Sanctions

Employees will be made aware of what conduct violates **Organization**'s established information security policies and procedures. These information security policies and procedures are set forth in this Manual. **Organization** will provide appropriate training to ensure that workforce members understand their roles and responsibilities.

Organization may supplement its information security policies and procedures in the form of verbal or written training, security news updates, and other measures. Workforce members are responsible for adhering to information security policies and procedures as set forth in this manual and these other sources.

To foster workforce awareness of conduct that may be subject to sanctions, **Organization** requires that all members of **Organization's** workforce sign a HIPAA *Confidentiality* form, upon hire, indicating that they have been informed, understand, and agree to abide by, **Organization's** security practices. Workforce members will also sign, upon hire, an attestation indicating that they understand the applicable parts of this manual. **Organization** will make every effort to ensure that training on its security policies and procedures is accurate and up-to-date. If, at any time, a workforce member is uncertain of how to perform a particular task or how to proceed, he or she should contact their supervisor or the Security Official for assistance.

Sanctions Procedures – Investigation:

Organization may learn of a potential violation of its security policies and procedures from patients, vendors, or members of the workforce. When a workforce member believes that a security policy or procedure violation has occurred, might have occurred, is occurring, or will occur, the workforce member should report the suspected violation or violation to their supervisor or to the Security Official, as established by **Organization**. The workforce member should state the nature of the suspected violation, including how the workforce member learned of it. **Organization** is prohibited from retaliating against a workforce member who has a good-faith belief that a security violation has taken place.

Organization will investigate all reported violations. Investigation may include interviews of witnesses or others who may have knowledge pertaining to the violation. The investigation will be promptly conducted. The Security Official will then determine whether a violation has occurred, and will document his or her findings and inform the appropriate individuals.

Procedures for Applying Sanctions:
If the Security Official has determined that sanctionable conduct has occurred, the Security Official may consider several criteria when determining the appropriate disciplinary measure.

- What was the intent of the person who committed the violation (e.g., was the violation intentional, or unintentional?)
- What is the risk to **Organization** resulting from the violation?
    - Is there a potential risk for patient harm?
    - Is there a risk of harm to **Organization**?
    - Is there a risk the public may be affected by the inappropriate use or disclosure?
- Has the employee or workforce member previously committed a violation(s)?
- What sanctions were applied for the previous violation(s)?
- What is the history of **Organization**'s sanctions for similar or identical infractions committed by *other* workforce members whose job roles or duties are the same as or similar to the workforce member?
- Are there mitigating circumstances that would support reducing any disciplinary/corrective action in the interest of fairness and consistency?

Once these criteria and any other pertinent information has been evaluated, the Security Official will impose a sanction if warranted. The Security Official will then document his or her findings and inform the appropriate individuals. Affected workforce members shall be informed of sanctions in writing.

Procedures for Documentation:
Organization will document all infractions, suspected infractions, investigations, and sanctions it has imposed. If investigation or other sanctions materials contain *ePHI* or PHI, **Organization** will comply with all Privacy Rule and Security Rule measures to ensure its protection. Documentation pertaining to proposed sanctions and their administration will be retained for a minimum of six years after its creation.

***Information system* Activity Review:**
Organization will regularly review records of *information system* activity, such as audit logs, *Access* reports, and security incident tracking reports. Such review is necessary to ensure that the *confidentiality*, *integrity*, and *availability* of *ePHI* is maintained.

Organization will review *Access* and activity logs to detect, report, and guard against the following:

1. Network vulnerabilities and intrusions.
2. Breaches in *confidentiality* and security of patient PHI.
3. Performance problems and flaws in applications.
4. Improper alteration or destruction of *ePHI* (information *integrity*).

This policy applies to ALL **Organizational** information applications, systems, networks, and any computing devices, regardless of ownership status (e.g., owned, leased, contracted, and/or stand-alone).

What are Log Review and Review Trail Activities?
Log review is the internal process of reviewing *information system Access* and activity (e.g., log-ins, file *Access*es, and *security incidents*). **Organization** will performic periodic reviews of system logs. **Organization** will also perform reviews as a result of a patient complaint, or when there is suspicion of workforce member wrongdoing. **Organization**, when performing reviews, will take into account the latest security risk analysis results.

Log review will consist of review of all system logs. System logs are records of activity maintained by the system which provide information that includes:

- The date and time of a system activity;
- The origin of a system activity;
- The identification of the *user* performing the activity; and
- A description of the attempted or completed activity.

A **review trail** is a means of monitoring operations to determine if a security violation occurred, by providing a chronological series of logged computer events, called system logs, that relate to an operating system, an application, or *user* activities. Review trails identify who (through identifying login ID and *password*) did what (created, modified, deleted, added, etc.), to what data, and when (date and time).

Procedure for Log Review:
Organization will assign responsibility for reviewing records of *information system* activity, such as audit logs, *Access* reports, and security incident tracking reports, to the Security Official. The Security Official must:

- Assign *Access* and activity log review to the individual(s) responsible for the specific applications, systems, or networks that must be reviewed. **Organization** must document the **Organization**'s, or individual names and job titles, of those responsible for *information system*s activity review, including login monitoring, and *Access* report preparation and review.
  The Security Official and/or or these assignees will periodically review *Access* and activity logs.

Procedure for Review Trails:
Review of address *Access* and activity logs will be performed at the following levels, listed below:

- **User:** *User* level review trails generally monitor and log all commands directly initiated by the *user*, all identification and *authentication* attempts, and files, patients, and resources *Access*ed.

- **Application:** Application level review trails generally monitor and log *user* activities, including data files opened and closed, patients *Access*ed, specific actions, and printing reports.
- **System:** System level review trails generally monitor and log *user* activities, applications *Access*ed, and other system defined specific actions.
- **Network:** Network level review trails generally monitor information on current operations, penetrations, and vulnerabilities.

Procedure: Evaluation and Reporting of Review Findings:

1. System logs that are routinely gathered will be reviewed periodically and as part of a risk assessment.
2. Written reports of review findings will be submitted to the Security Official.
3. Whenever indicated through evaluation and reporting, appropriate corrective actions must be undertaken. These actions will be documented and shared with the responsible and sponsoring departments/units.
4. If criminal activity is discovered during a review, it should be reported to appropriate law enforcement.

Review Log Security Controls and Backup:

1. Review logs will be protected from unauthorized *Access* or modification, so the information they contain will be available if needed to evaluate a security incident.
2. Whenever possible, audit trail information will be stored on a separate system. Separate system storage will allow **Organization** to detect hacking *security incidents*.
3. Review logs maintained within an application will be backed up as part of the application's regular backup procedure.
4. **Organization** will review internal back-up, storage and data recovery processes to ensure that the information is readily available in the manner required.

Retention of Review Information:

Systems and data *Access* logs must be retained for a minimum of six years. Network device and systems logging (e.g., firewall logs, switch logs, wifi logs) will be retained for a minimum of one year.

RELEVANT HIPAA REGULATIONS:

- §164.308(a)(1)(ii)(A) *Risk analysis*
- §164.308(a)(1)(ii)(B) *Risk management*
- §164.308(a)(1)(ii)(C) *Sanction policy*
- §164.308(a)(1)(ii)(D) *Information system Activity Review*

Security Policy 3.0 Workforce Security

FULL POLICY LANGUAGE

Policy Purpose:

Organization has adopted this policy to ensure that all workforce members have appropriate *Access* to *ePHI*, and to ensure that workforce members who are not authorized to *Access ePHI* are prevented from obtaining such *Access*.

Policy Description:

This policy covers the procedures that **Organization** has implemented to ensure that workforce *Access* to *ePHI* is authorized, supervised, and appropriate. This policy ensures that **Organization**'s rules for *Access* to electronic protected health information are consistent with the requirements of the HIPAA Privacy Rule. The policy sets forth a series of *Access* controls that reasonably and appropriately restrict *Access* to only those persons and entities with a need for *Access* to *ePHI*.

Procedure to Ensure That *Access* to *ePHI* is Appropriate

To ensure that members of the workforce have appropriate *Access* to *ePHI*, **Organization** will document the names, job roles, and appropriate levels of *Access* to *ePHI* to which each workforce member has been assigned.

Workforce Security consists of three components:

1. Authorization and Supervision.
2. Workforce Clearance Procedure
3. Termination Procedure

Authorization and Supervision:
To ensure that members of the workforce have appropriate *Access* to *ePHI*, **Organization** will maintain documentation that contain the names of employees, their job descriptions, and the appropriate level of *Access* to *ePHI* to which each employee has given, based on their job role.

Organization will make workforce members aware of the identity, roles, and responsibilities of their supervisors. **Organization** will inform individuals as to who is responsible for supervising workforce members who work with *ePHI*, or who work in locations where it might be *Access*ed.

Staff, employee and workforce members' duties will be separated so that only the minimally necessary *ePHI* based on the specific job description is made available upon request.

Minimum Necessary *Access*:
Organization will ensure that only those workforce members who require *Access* to *ePHI* are granted such *Access*. The supervisor or Security Official will grant only that level of *Access* that is the minimum necessary amount of *Access* required to perform each workforce member's job role and responsibilities. If a workforce member no longer requires *Access*, it is the supervisor or Security Official's responsibility to complete the necessary process to terminate *Access*.

The Security Official will provide formal written and documented authorization before granting *Access* to sensitive information.

Authorization and Supervision: Procedures
Organization uses the following procedures to determine which individuals are authorized to work with *ePHI*:

- Determination of the appropriate *Access* level for each workforce member.
- Maintenance of a list detailing the level of authorization for each workforce member.
- Assigning a unique name or number for identifying and tracking computer network *user*s' identities.
- Assignment of *user* IDs or logon accounts only with prior with management approval.

- Requiring all *user*s to work from standard *user* level accounts. Even administrative personnel should work from standard accounts and escalate privileges to install apps or modify the system.
- Training of all workforce members regarding their individual appropriate *Access* authorization, what such authorization permits, and what it prohibits.

Security Awareness Prior to Getting *Access*:
Before **Organization** grants *Access* to any of the various systems or applications that contain *ePHI*, **Organization** will train workforce members minimum standard. Topics that are covered in training include:

1. Proper uses and disclosures of the *ePHI* stored in systems or application(s);
2. How to properly log on and log off the systems or application(s);
3. Protocols for correcting *user* errors (i.e., inadvertent alteration or destruction of *ePHI*);
4. Instructions on contacting a designated person or help desk when *ePHI* may have been altered or destroyed in error; and
5. Reporting a potential or actual security breach.

Organization will inform workforce members that *Access* to the *information system* or application may be revoked or suspended, consistent with **Organization's** privacy and security policies and practices, if it has been determined that a workforce member has engaged in unauthorized *Access*.

Visitors, Contractors, and Business Associates:
To prevent those personnel who do not have *Access* to *ePHI* from obtaining such *Access*, **Organization** requires the following:

- All visitors must sign in and out.
- All vendors who have a BAA signed with **Organization** must sign in and out. Business associates may sign out a visitor badge to temporarily *Access* facilities, if needed.
- All contractors who have not signed a BAA with **Organization** must sign in and out at the front desk. **Organization** may provide contractors with a badge for temporary *facility Access*, should contractors choose to provide the front desk with photo ID.

Workforce Clearance Procedure Policy:
Organization will periodically determine whether a workforce member's *Access* to *ePHI* is appropriate. In doing so, Organization will review role definitions and assignments for appropriateness, at least annually.

Background Checks:

Organization will check all potential hires, new hires, and current employees against the HHS Office of Inspector General's List of Excluded Individuals/Entities (LEIE). https://oig.hhs.gov/exclusions/exclusions_list.asp

Organization will assess risk, cost, benefit, and feasibility as well as other protective measures in place, in deciding whether more detailed screening is appropriate. Background checks and screening will be conducted in accordance with federal, state, and local laws, regulations, and ordinances.

Restriction of *Access* to *ePHI*:
Organization will restrict *Access* to *ePHI* when appropriate. Restrictions are dependent upon job responsibilities and the amount and type of supervision required. Restrictions must be in accordance with the requirements of the Privacy Rule minimum necessary standard when applicable. See *Privacy Policy 3.0, Minimum Necessary Standard*. Clearance controls depend upon the type of workplace. For example, a personal clearance may not be reasonable or appropriate for a small provider whose only assistant is his or her spouse.

Workforce Clearance Procedures – Granting *Access* to *ePHI*:
Workforce clearance procedures consist of the following:

- **Screening of Workforce Members Prior to *Access*:** The supervisor or Security Official will ensure that information *Access* is granted only after verifying that the *Access* of a workforce member to *ePHI* is necessary and appropriate.
- **Training of Workforce Members: Organization** will train workforce members on **Organization**'s HIPAA Privacy and Procedure Manual and HIPAA Security Policy and Procedure Manual.
- **Signing a Confidentiality Agreement:** Prior to, and as a prerequisite to, being issued a *User* ID or logon account to *Access* any *ePHI*, each workforce member will sign **Organization's** *Confidentiality* Agreement. Workforce members will thereafter comply with all of **Organization's** security policies and procedures.

Security Official and Supervisor Responsibilities:
- The Security Official will ensure a periodic review of, and update as appropriate, *Access* authorization levels and personnel clearance levels (together "Levels"), to ensure that the *Access* of a workforce member to *ePHI* is appropriate.
- When adding, modifying, or canceling security clearance *Access*, the Security Official will update the personnel clearance and *Access* authorization levels accordingly.
- Supervisors will notify workforce members of any changes to their *Access* or clearance levels.

Termination Procedures:
Organization will terminate *Access* to *ePHI* when the employment of, or other arrangement with, a workforce member ends, or when **Organization** determines that it is not appropriate for a certain workforce member to have *Access* to *ePHI*.

Circumstances When Termination of *Access* is Required:
Department managers or their designated representatives **must** terminate a workforce member's *Access* to *ePHI* in these circumstances:

1. If management has evidence or reason to believe that the *user* is using *information system*s 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.

Specific Termination Procedures:
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 *user*s and *password*s; and
- Completion of an employee termination 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.

Organization will document termination procedures and measures.

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*

Security Policy 4.0 Information *Access* Management

FULL POLICY LANGUAGE:

Policy Purpose:

This policy sets forth procedures for **Organization** grants workforce *Access* to *ePHI*. The policy further sets forth how **Organization** documents, reviews, and modifies a *user*s' *Access* rights to *ePHI*.

Policy Description:

This policy contains **Organization**'s procedures for authorizing *user Access* to *ePHI*. These procedures are referred to as "*Access* control procedures." **Organization** will authorize *Access* privileges through a documented process that establishes the identity and role of the *user*, and the extent of the need to *Access* the *ePHI*. **Organization** will establish, document,

review, and modify *user Access* rights to ensure that the appropriate level of *Access* is granted at all times.

Organization's *Access* control policies and procedures will reasonably and appropriately restrict *Access* to only those persons and entities with a need for *Access* to *ePHI*. "*Access*" may consist of *Access* to *workstation*s, programs and other processes that may display, contain or process *ePHI*. The purpose of these procedures is to limit inappropriate or unnecessary workforce *Access* to, use of, and disclosure of protected health information. Such *Access*, use, or disclosure may violate the HIPAA Privacy Rule, which prohibits unauthorized *Access*, use, or disclosure.

Organization will require that employees who need *Access* to adhere to "least privilege," which means that *user*s may *Access* only that *ePHI* that is necessary to perform their job functions, and no more.

***Access* Authorization Policy:**
Organization will, when required, authorize *user Access* to *ePHI* - for example, through *Access* to a *workstation*, transaction, program, or process. As part of this system, **Organization** will use an account request form requiring management approval. *Access* will be granted in accordance with a role-based approach.

***Access* Authorization-Procedures:**

- Upon hire of new workforce members, **Organization** will document the names and job functions of the workforce members.
- **Organization** will require new workforce members to complete an *Access* Request form (to be provided by **Organization**) to establish the appropriate level of *Access*.
- **Organization** will review the *Access* request form to determine what level of *Access* is appropriate.
- **Organization** will ensure that workforce members are trained during their orientation, to include information on the degree of *Access* permitted by their job functions, and to understand what unauthorized *Access* is and how it is prohibited.
- **Organization** will ensure that only authorized workforce members may install any software, and that any software they install must be approved by the Security Official.
- **Organization** will train the workforce that *user*s are prohibited from connecting their personal portable devices to any *workstation*s or devices on the **Organization**'s internal network.
- **Organization** will train the workforce that only approved personal portable devices can *Access* the internal network
- Training will also emphasize that *user*s are prohibited from sending *ePHI* through any unapproved system or service (e.g., file sharing applications, unencrypted/personal email).
- **Organization** will provide the following additional training
    1. Training on proper uses and disclosures of *ePHI*.

2. Training on how to properly log on and log off applications.
3. Instructions for contacting a designated person or help desk when *ePHI* may have been altered or destroyed in error; and
4. Training on how to report a security incident.
5. Antiphising training.
6. Cybersecurity training.

Once training has been completed, workforce members may begin to *Access ePHI* to perform work, in accordance with **Organization**'s *Access* level determination. **Organization** will document all *Access* request forms, all levels of *Access* determinations, and all training.

***Access* Establishment and Modification – Policy:**

Organization, using its access authorization procedures, will establish, document, review, and modify a *user*'s right of *Access* to *ePHI*. Organization will do so in accordance with the principle of "least privilege," which means that *user*s may *Access* only that *ePHI* that is necessary to perform their job functions. **Organization** will ensure that *Access* and *Access* levels are regularly reviewed for appropriateness. **Organization** will require prompt initiation of account termination or modification.

***Access* Establishment and Modification – Procedures:**

- **Organization will determine who will establish and modify *Access*.**
- **Organization** will create and maintain *Access* control lists such that:
    - Appropriate authorizations are upheld; and
    - Clearance levels of workforce members and other *user*s support the privileges granted.
- **Organization** will regularly review *Access* rights for each individual, to ensure such rights are current and appropriate.
- **Organization** will, as appropriate, modify *Access* control lists to reflect status changes or disqualifying factors, such as termination, lapses in required training, or job function (i.e., authorization) changes. **Organization** will then implement appropriate *Access* control changes.
- If a workforce member transfers to another program or changes role(s) within the same program within **Organization, Organization:**
    - Will promptly evaluate the workforce member's current *Access*.
    - Will follow procedures for requesting and granting *Access* to *ePHI*. commensurate with the workforce member's new role and responsibilities.
    - Will implement appropriate *Access* control changes.
- **Organization will, at all times, restrict the administrative group *Access* for all systems (computers, servers, routers, firewalls, etc.) to workforce or entities approved by the Security Official.**

Ongoing Compliance for *Access*:

To ensure that workforce members have *Access* to *ePHI* only when it is required for their job function, Organization will do the following:

- When a workforce member changes roles, the Security Official will evaluate their *Access* to *ePHI* and revise as necessary.
- The supervisor or Security Official will deactivate the accounts of workforce members or entities who have the accounts of members who leave the workforce or entities with whom **Organization**'s relationship has been terminated.
- The supervisor or Security Official will also deactivate an account when the results of a risk analysis call for that measure.

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*

Security Policy 5.0 Security Awareness and Training

FULL POLICY LANGUAGE:

Policy Purpose:

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

Policy Description:

Security Awareness and Training:

Security awareness and training is key to eliminating **Organization's** exposure to both malicious threats and accidental errors or omissions. Training will consist of security updates and reminders; procedures on protection from *malicious software*; procedures for monitoring log-in attempts and reporting discrepancies; and procedures for creating, changing, and safeguarding *password*s.

Organization utilizes a security awareness and training program for all members of the workforce (including management). **Organization** will require *user*s to complete security training and attestation in The Guard at least on hire, and annually for all employees. **Organization** will document all attestations. Attestations are employees' attesting to understanding **Organization**'s security policies and procedures.

Security Awareness and Training – Periodic Security Updates:

- **Organization** will provide the workforce with periodic security notices and updates regarding current security threats to *ePHI* such as malware or phishing schemes that are occurring or have recently occurred within **Organization**.
- **Organization** will also periodically notify the workforce of **security changes** that **Organization** has recently made. Such changes may include changes to security policies or procedures, or changes to security protocols (such as a change to how employees leaving work for the evening should secure laptops containing *ePHI*).
- **Organization** will provide periodic reminders about the importance of security awareness in the context of HIPAA. **Organization** will provide such reminders through periodic newsletters, email, video, or webinar reminders.
- **Organization** will review and train employees on changes to internal security policies, internal security procedures, and technologies, as part of an annual process.

Policy for Training on Protection from *Malicious software*:

Organization deploys *malicious software* checking programs on all systems containing *ePHI*. Organization will keep licenses for this software up-to-date. Organization will keep the applications up to date. Members of the workforce may not bypass or disable antimalware software or *malicious software* checking programs, unless properly authorized to do so.

General *Malicious software* Training:

Organization will periodically train the workforce on the following subjects related to *malicious software*:

- Potential harm that can be caused by malware.
- Malware prevention, and how malware prevention software works.
- Phishing and how to prevent it.
- How to detect *malicious software* programs.
- How to appropriately use software.
- How to identify and protect data, when possible, against malicious code and software.

All training will be documented.

Specific Protection from *Malicious software* and Training:
Organization utilizes measures for guarding against, detecting, and reporting *malicious software*. Examples of such measures include endpoint protection (AV/Antimalware), *encryption* of data in transit and at rest, and reporting and addressing *security incidents* and breaches. Specific measures include:

- **Organization** will require installation of operating system and third party application updates (patches) and keep them current. In some small environments, automatic updates may be sufficient for addressing this control. **Organization** will require changing or removing default logins and *password*s. Examples of systems and devices that require *password* changes include:
    - Routers
    - Firewalls
    - Network switches
    - Wireless *Access* points
    - Internet of Things (IOT) devices
    - *Access* control systems, etc.
- **Organization** will require the disabling of unnecessary services on all computer systems.
- **Organization** will require periodic installation and updates of malware protection software.
- **Organization** will set proper file/directory/ownership/permissions to enforce "need to know *Access* levels for all workforce members.
- **Organization** will require regular (no less than annual) review of HIPAA *workstation* browser settings to ensure that these settings comply with **Organization**'s recommended browser security settings.
- **Organization** will perform periodic (no less than annual) review of email client settings to ensure these comply with **Organization**'s current email client settings.
- **Organization** will perform periodic network vulnerability scans of systems containing known *ePHI* and *workstation*s that *Access ePHI*, and take adequate measures to correct vulnerabilities that **Organization** discovers
- **Organization** will implement email malicious code filtering.
- **Organization** will install and enable network firewalls to reduce the threat of unauthorized remote *Access*.
- **Organization** will install intrusion detection software (IDS) and/or systems to detect the threat of unauthorized remote *Access*.
- **Organization** will train employees on the above measures.

Procedures for Monitoring Login Attempts and Reporting Discrepancies:

Log-in Monitoring:

Organization has the right to monitor system *Access* and activity of all workforce members. All network devices (firewalls, customer managed routers, wifi equipment, and switches) will be configured to capture and retain *Access* and activity logs, including failed logons and attempted attacks.

To ensure that *Access* to servers, *workstation*s, and other computer systems containing *ePHI* is appropriately secured, **Organization** will implement the following measures:

- **Organization** will require activation of *user Access* logging for all systems (hardware or software) with *Access* to *ePHI*.
- **Organization**, as part of a risk assessment or as otherwise required by the HIPAA Security Rule, will periodically review *Access* logs and activity reports and logs. As part of this review, **Organization** will document any repeated failed login attempts on each system or device containing *ePHI*, and identify any patterns of suspicious activity.
    - All failed login attempts of a suspicious nature, such as continuous attempts, will be reported immediately to the Security Official.
    - Discovery of repeated failed login attempts will result in disabling of *user* accounts or other appropriate measures.

Procedures for Creating, Changing, and Safeguarding *Password*s:
Organization will require creation, changing, and safeguarding of strong passwords, and will train employees on password creation, change, and safeguarding. All passwords will meet NIST or ISO *password* guidelines. Per NIST guidance, a strong *password* consists of:

- A minimum of eight characters and a maximum length of at least 64 characters.
- The ability to use all special characters but no special requirement to use them
- Restriction of sequential and repetitive characters (e.g. 12345 or aaaaaa).
- Restriction of context-specific *password*s (e.g. the name of the site, etc.).
- Restriction of commonly used *password*s (e.g. p@ssw0rd, etc.) and dictionary words.
- Restriction of *password*s obtained from previous breach incidents.

Workforce members will use a *password* management solution. This means workforce members will either:

- Commit *password*s to memory, or,
- Store *password*s in an **Organization**-approved credentials management system.

Additional *Password Security measures*:
- **Organization** prohibits the sharing of *password*s. Workforce members may not share *password*s with other employees, managers, visitors, family members, friends, or anyone else. Workforce members who suspect that their *password* has become known by another person shall change their *password* immediately.

- **Organization** will enforce the following additional *password* protection requirements for *user*s:
    - Never reveal a *password* over the phone to anyone.
    - Never reveal a *password* in an email message.
    - Never reveal a *password* to your supervisor.
    - Never talk about a *password* in front of others.
    - Never hint at the format of a *password* (i.e., "my family name").
    - Never reveal a *password* on questionnaires or security forms.
    - Never share a *password* with family members.
    - Never reveal a *password* to co-workers.
    - Never write down your *password*.
    - Never keep a list of *user* IDs and *password*s in your office.
    - Never misrepresent yourself by using another person's *user* ID and *password*.

Frequency of Security Awareness Training:
Organization will ensure that all new members of the workforce receive security awareness training. New or additional security training will be provided to appropriate staff when changes occur in either technology or practices, or when **Organization** has determined that additional or refresher training is appropriate. All training will be documented.

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*

Security Policy 6.0 Incident Response & Reporting

FULL POLICY LANGUAGE:

Policy Purpose:
Organization will identify, report, and respond to suspected and known *security incidents*; will mitigate (to the extent practicable) the harmful effects of *security incidents* that are known; and document *security incidents* and their outcomes. In addition to this policy, please also refer to Security Policy 20.0 and Security Policy 21.0. The policies provide additional information related to *security incidents* and to breaches of unsecured PHI.

Policy Description:
The HIPAA Security Rule defines a "security incident" as the attempted or successful unauthorized *Access*, use, disclosure, modification, or destruction of information or interference with system operations in an *information system*.

Organization's security incident response and reporting mechanism covers:

- What specific actions are considered to be *security incidents*;
- How will incidents be documented, reported, and investigated
- What information should be contained in the documentation;
- What are the appropriate administrative responses to incidents
- What are the appropriate technical responses to incidents.

See also Security Policy 20.0 for additional information about incident response and reporting, including for breaches of ePHI.

Procedure: Identification and Determination of *Security incidents*
In determining what constitutes a security incident, **Organization** will rely upon the information gathered in complying with the other security standards - for example, its risk analysis and risk management procedures and the Privacy Rule standard. **Organization** will then determine what specific actions would be considered *security incidents*,

Examples of *Security incidents* Include:

- Computer system intrusion, including ransomware attacks.
- Unauthorized *Access* to data, applications, or accounts.
- Unauthorized changes to computers or software.
- Loss or theft of electronic media or computer systems.

How are Incidents Documented, Reported, and Investigated?
A workforce member who becomes aware of a security incident should report the incident to his or her supervisor or to the Security Official, as soon as possible. Workforce members should try to report incidents outside the presence of other workforce members and individuals.

Once the workforce member has notified the supervisor or Security Official, the supervisor or Security Official should record the following information in a log (See Policy 20.0: Recordkeeping).

- Date and time of the incident.
- Detailed description of the incident.
- Any further information, such as unusual activities or individuals associated with the incident.

The supervisor or Security Official will determine whether immediate action is appropriate. Such appropriate immediate actions may include disconnecting, disabling, or otherwise securing compromised devices or media

While the supervisor or Security Official takes appropriate actions, **Organization** should attempt to avoid making any updates or other modifications to software, data, or equipment involved or suspected of involvement with a security incident. Such modifications should ideally be made only after appropriate investigation and remediation of *security incidents*.

Once an incident is reported/recorded, the supervisor or Security Official, will investigate the reported incident. If the incident includes PHI that is not *ePHI*, the Security Official will coordinate with the Privacy Official to address the incident together. While the supervisor or Security Official is investigating, the Security Official may, if appropriate, restrict workforce *information system Access* or operations to protect against unauthorized information disclosures.

As part of the investigation, the supervisor or Security Official may require the assistance of other members of the workforce, who are expected to cooperate fully.

What Information Should be Contained in Documentation?
Organization, as it investigates, will document its identification of all system-related information, such as:

- 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 its determination of which systems were impacted, and which levels of privilege were *Access*ed.

Organization will also document:

- How widespread the vulnerability is.
- How far into the internal systems the intruder/attack got.
- Which systems have been compromised.
- Any risk to *ePHI* stored by any systems.

What are The Appropriate Administrative Responses to Specific Incidents?
If the Security Official concludes that applicable federal or state laws or regulations may have been violated, **Organization** will consult with legal counsel and any other appropriate personnel to determine whether law enforcement notification or other notification is required.

If the Security Official concludes that there is a possibility of unauthorized *Access* to *ePHI*, the Security Official will notify the Privacy Official. **Organization** will utilize the HIPAA Incident Assessment Tool and the Unsecured PHI Job Aid, in addressing the incident. If any disciplinary action is warranted, refer to Security Policy 2.0, *Security Process Management*.

Organization will use feedback process to ensure that those reporting incidents are notified of results after the incident has been remedied and closed.

What are the Appropriate Technical Responses to Specific Incidents?
The results of the investigation may require **Organization** to implement mitigation or remediation measures, as appropriate. Such measures may 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 of data from approved backups.
- Restoration of systems that were brought offline during incident response,.
- Monitoring of affected systems and infrastructure for similar, subsequent incidents. If such monitoring reveals the occurrence of recurring or high-impact incidents, **Organization** will consider implementing or strengthening appropriate controls to limit the frequency, damage and cost of future occurrences.

Training and Documentation:
Organization will train all workforce members on their roles and responsibilities related to incident response. If you do not understand your responsibilities, please consult your supervisor or the Security Official. Documentation of all training, security incident reports, investigations, and disciplinary measures will be maintained for a minimum of six years.

RELEVANT HIPAA REGULATIONS:

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

Security Policy 7.0 Contingency Plan

FULL POLICY LANGUAGE:

Policy Purpose:
To outline how emergency response procedures are to be created, implemented, and maintained.

Policy Description:

Organization will utilize contingency plans, which set forth how **Organization** will respond to emergencies and disasters.

During emergencies or disasters, systems containing *ePHI* may be damaged. **Organization**'s contingency plans will ensure that **Organization** is prepared for an emergency, and that, if an emergency strikes, **Organization** will be able to continue as many critical operations as possible.

These contingency plans consist of:

- A Data Backup Plan;
- A Disaster Recovery Plan; and
- A Business Continuity Plan (Emergency Mode Operation Plan).

Data Backup Plan:

Organization will create a data backup plan, under which **Organization** will perform backups of electronic *information system*s and devices on a regular basis. The backup frequency schedule will be based on the potential risks and impacts of data loss, as determined by the security risk analysis. **Organization** will periodically test the plans on no less than an annual basis. **Organization** will revise the plan when there has been a change in business needs or technology requirements.

Organization will implement backups for all physical storage targets containing *ePHI* (computer systems, server systems, physical media, and external hard drives) to create and retrieve exact copies of *ePHI*. **Organization** will hold these backups held offsite in a secure location, or with a HIPAA-compliant cloud vendor.

Organization will implement backups for all cloud storage targets (Google, Microsoft 365, Dropbox, etc.) to create and retrieve exact copies of electronic protected health information.

Backup Procedures:

1. **Organization** will create and maintain retrievable exact copies of *ePHI* and other data necessary for the operation of its electronic *information system*s.
2. All backups will contain sufficient information to be able to restore the *information system* to a recent, operable, and accurate state.
3. Backups will be performed in a systematic manner in accordance with established backup strategies and procedures outlined in the Business Continuity Plan (see Security Policy 7.0, *Contingency Plans*, below, for information about the business continuity plan).
4. All backup media will be stored in a location that is secure.
5. All backup media will be stored in a separate location from the *information system* from which the backup was created.
6. **Organization** will maintain accurate and complete records of existing backups. These records will include the location of all backup media.

7. **Organization** will document backup activity and backup files.
8. **Organization** will revise its data backup plan when called for by the results of a risk analysis or change in the operating environment. The Security Official will approve and document all revised backup plans and ensure that these plans are implemented and disseminated to the workforce.

Disaster Recovery Plan:
Organization will utilize Disaster Recovery Plan, which outlines procedures to restore the loss of data in the event of an emergency. This written Disaster Recovery Plan will ensure that **Organization** can recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster affecting systems containing *ePHI*.

Disaster Recovery Plan Components:
Organization's HIPAA disaster recovery plan requires **Organization** to establish, and implement as needed, procedures to restore any loss of data. Best practices for disaster recovery plan creation indicate that the plan should contain at least the following components:

- **A communication plan:** A disaster recovery plan should contain a procedure for how employees are to communicate with other employees, and with management, in the event of a disaster. The plan should indicate how a disaster should be reported, and who should be notified of a disaster. The plan should include employee contact information to allow for prompt reporting and notification.
- **Role description:** The plan should also describe each employee's role in the days following the disaster. The plan should designate employee assignments, such as who will assess damage, and who will have overall responsibility for systems recovery.
- **A detailed asset inventory**: The HIPAA disaster recovery plan should contain a detailed inventory of all computer *workstation*s and their components, as well as scanners, tablets, phones, and printers that are regularly used by staff.
- **An equipment plan:** Desktop computers, laptop computers, portable devices, printers, and other computer equipment can be damaged in the event of major storms, blackouts, or earthquakes. The HIPAA disaster recovery plan should describe how this equipment should be protected in the event of a disaster. This description should consist of various steps. For example, to prevent water damage, equipment should first be moved off the floor, then (if possible) moved into a room or area with no windows, and then, the equipment should be wrapped securely in plastic or other material to prevent water from getting in.
- **A data restoration priority plan:** The Disaster Recovery Plan will include procedures to Recovery Plan will provide procedures for recovery of any loss of *ePHI*, and will indicate the systems needed to make that *ePHI* available in a timely manner. The Disaster Recovery Plan will include procedures to log system outages, failures, and data loss to critical systems. The plan will outline what *ePHI* from data

backups should be restored first in the event of a disaster, to ensure *ePHI* is made available in a timely manner. The plan will then outline the remaining order of priority for data restoration. Prioritization should reflect both legal and business concerns. Data required by law to be maintained or secured, such as PHI in the case of HIPAA, and injury and illness records in the case of the Occupational Safety and Health Act ("OSH Act") should be prioritized for recovery. Restoration of data – such as billing information and online appointment calendars – that is necessary for the business to continue at a minimum level of service, should also be prioritized.

- **A vendor communication and service restoration plan:** When the disaster is over, you will want to restore services as quickly as possible. This requires prompt communication with vendors such as phone and internet providers, and electricity providers. The HIPAA disaster recovery plan should contain the contact information of all vendors, along with a description of when and how (e.g., telephone, Internet) each vendor is to be contacted.
- **Plan Storage, Training, and Review: Organization** should ensure that the disaster recovery plan is made available to employees, and ensure that the plan is *Access*ible at more than one location. **Organization**, if it is a single location, should store a copy of the plan at an offsite location. Employees should know where the offsite location is. In addition, **Organization** should conduct periodic training on the disaster recovery plan so employees will know what is expected of them under the plan. **Organization** will test the disaster recovery restore *ePHI* from data backups in the case of a disaster causing data loss. **Organization** will review the Disaster procedures outlined in the Disaster Recovery Plan on a periodic basis to ensure that *ePHI* and the systems needed to make *ePHI* available can be restored or recovered.

Emergency Mode Operation Plan Procedures:

- **Organization** will implement a written business continuity plan (emergency mode operation plan), and update it as necessary. The plan will contain procedures to enable continuation of critical business processes for the security of *ePHI* while **Organization** is operating in emergency mode.
- **Organization** will test emergency mode operation procedures on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode.
- **Organization** will submit any proposed revisions to the Emergency Mode Operation Plan to the Security Official for approval.

Procedures for Periodic Testing and Revision of Contingency Plan:

The data backup plan, disaster recovery plan, and business continuity plans will all contain procedures for periodic plan testing and revision:

- Each plan will be tested no less than annually. Each plan will also be tested whenever material modifications are made to the plan, to substantiate that the modified plan is effective. Testing will include training of workforce members, to ensure they understand their plan 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 media testing is an important component of plan testing. **Organization** will ensure that backup media will be tested periodically for readability. If there are readability issues, backup media will be replaced to ensure sufficient backup data is available enable the restoration of the system to a recent, operable, and accurate state.

Applications and Data Criticality Analysis:
Organization will require the assessment of the relative criticality of specific applications and data in support of other business continuity plan components. To perform this assessment, complete Steps #1-6 of the risk analysis procedure. The results will indicate which systems and information require recovery prioritization. Prioritization of critical systems and information will help identify where to focus planning efforts.)

Organization will periodically perform the data and application criticality assessment no less than annually to ensure that appropriate procedures are in place for data and applications at each level of risk.

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*

Security Policy 8.0 Monitoring and Effectiveness

FULL POLICY LANGUAGE

Policy Purpose:

Organization will perform periodic security assessments to ensure **Organization** is complying with the HIPAA Security Rule. This policy describes how these assessments will be performed.

Policy Description:

Organization will perform a periodic technical and non-technical security evaluation that establishes the extent to which **Organization**'s policies and procedures meet the requirements of the HIPAA Security Rule.

Organization will perform the evaluations in response to environmental or operational changes affecting the security of electronic protected health information (*ePHI*). Examples of changes include changes in the operating environment (e.g., security-related regulations and laws, new threats, occurrence of security violations, breaches of unsecured PHI, and other *security incidents*), and changes in operations (e.g., changing of business practices, upgraded or new technology).

The evaluation will encompass all **Organization**al safeguards and systems, as well as a review of *information systems*. **Organization** will either perform the evaluation using its own workforce, or have the evaluation be performed by an outside **Organization**.

Organization, based on the results of the evaluation, will update its *security measures* to remediate flaws revealed by the assessment.

Procedure: Evaluation

Organization will identify and document who is responsible for determining when evaluation is necessary due to environmental or operational change. **Organization** will identify who will perform the evaluation.

As part of the evaluation, **Organization** will:

- Determine whether security controls are correctly implemented, and whether these control, as implemented, are effective in their application.
- Identify any new risks.
- Conduct reviews of the *facility*'s physical environment *security measures*.
- Conduct reviews of *workstation* use and security controls.
- Conduct reviews of device and media controls.
- Conduct reviews of *Access* controls, audit controls, *integrity* controls, identity and *authentication* controls, and transmission security controls.
- Conduct reviews of all security management process controls, information *Access* management controls, incident response and reporting measures, and contingency plans.

Organization will then decide how updates based on those evaluations are to be made (e.g., which authorized personnel may perform the updates, who may update what, what is

the update completion schedules). Any updated *security measures* must be sufficient to reduce risks and vulnerabilities to a reasonable level.

Organization will ensure that all evaluations, updates, and changes to policies and procedures are appropriately documented. **Organization** will establish an effective date for updated policies and procedures, and will then promptly disseminate updated policies and procedures to workforce members.

RELEVANT HIPAA REGULATIONS:

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

Security Policy 9.0 Business Associate Relationships

FULL POLICY LANGUAGE

Policy Purpose:

To provide rules for determination of what constitutes a business associate, to provide rules for creation, review, and termination of Business Associate Agreements.

Policy Description:

Business Associates:
A business associate is any person or entity that **Organization** hires, per a written agreement, to help **Organization** to do something. The "something" under the contract involves the business associate's creating, transmitting, receiving, or maintaining PHI or *ePHI* on or behalf of **Organization**. When **Organization** contracts with a business associate for the business to provide PHI-related services to **Organization**, **Organization** and the business associate must enter into a business associate agreement, using the following procedure:

The Security Rule at 164.314(a) outlines what must be in a business associate agreement. The business associate agreement must provide that the business associate, in the performance of its duties under the contract, will adequately safeguard ePHI it creates, receives, transmits, or maintains on **Organization's** behalf.

Procedure: Determination of When a Business Associate Agreement is Needed

1. **Organization** will review all contracts with vendors, suppliers, and other businesses, to determine if the contracts require a Business Associate Agreement ("BAA") with a business associate**. Organization** may permit a business associate to create, maintain, receive, or transmit *ePHI* on its behalf, only if **Organization** obtains satisfactory assurances, in the form of a documented written business associate agreement (BAA), that the business associate will appropriately safeguard the information. If a BAA is required, the business associate's contract managers must complete the BAA, and then return that BAA to **Organization** for **Organization's** approval and signature.
2. **Organization** will audit a prospective business associate's security posture via electronic questionnaire, known as a due diligence questionnaire. If the prospective business associate does not, based on its responses, provide satisfactory assurances that it will safeguard the *confidentiality*, *integrity*, and *availability* of PHI and *ePHI*, **Organization** will, in its discretion, permit the prospective business associate the opportunity to bring its practices in line with the Security Rule. If the prospective business associate does not provide the required assurances, **Organization** will not enter into a business associate agreement with the prospective business associate.
3. Once a prospective business associate has successfully completed the due diligence questionnaire, **Organization** will enter into a business associate agreement with that **Organization**.
4. **Organization** will ensure that the Business Associate Agreement includes certain required language. Under a Business Associate Agreement, a business associate subcontractor must provide that it will:

i. Implement and follow policies and procedures that address the HIPAA Security Rule's administrative, physical and *technical safeguards*, and other Security Rule requirements.
ii. Ensure that all business associate employees receive HIPAA security training on how to protect *ePHI*.
iii. Perform a detailed HIPAA risk analysis to determine whether PHI and *ePHI* are being properly safeguarded.
iv. Ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of the Security Rule, by entering into a business associate agreement with the business associate. In other words, a business associate must enter into a business associate subcontractor agreement with subcontractors who seek to perform functions involving creation, maintenance, transmission, and/or receipt of PHI on behalf of the business associate.
v. Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information, as required by the Breach Notification Rule.

5. After the business associate agreement has been executed, **Organization** will periodically conduct a security audit of the business associate's HIPAA Policies and Procedures as a means of due diligence, to ensure that the business associates subcontractor is taking the necessary precautions under the HIPAA Security Rule to protect the data that is shared with it.

Business Associate Non-Compliance:

1. If **Organization** knows of any activity, practice, or pattern of activity or practice of the Business Associate that constitutes a material breach or violation of an obligation under the contract or other arrangement, **Organization** will, as a first resort, take reasonable steps to repair the breach or end the violation, as applicable. Such steps include working with, and providing consultation to, the Business Associate.
2. If such steps are unsuccessful, **Organization** must terminate the contract or arrangement, if feasible. If termination is not feasible, Organization mist report the problem to the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) within 30 days of the incident.

Tracking and Identifying Business Associate Subcontractor Relationships:
Whenever **Organization** enters into a business associate agreement, **Organization** will notate the date of agreement and name of the business associate in a contract record or log. **Organization** will update the record each time a business associate relationship is formed or terminated.

Response to Complaints about Business Associates:

A workforce member of **Organization** may receive a report or complaint, from any source, about the business associate's inappropriately or inadequately, safeguarding ePHI. When an **Organization** workforce member receives a report or complaint, the workforce member will promptly provide information regarding that report or complaint to the Security Official. The Security Official will coordinate with **Organization**'s contract administrator or manager to document the alleged violation, and determine if remediation is required for the Business Associate subcontractor to attain/retain contract compliance.

RELEVANT HIPAA REGULATIONS:

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

Security Policy 10.0 *Facility Access* Controls

FULL POLICY LANGUAGE

Policy Purpose:

To provide for limitation of physical access to **Organization's** electronic *information system*s and the *facility* and facilities in which they are housed, while ensuring that properly authorized *Access* is allowed.

Policy Description:

This policy sets forth the *facility access controls* **Organization** will use to safeguard *ePHI* from any intentional or unintentional use or disclosure. These controls allow **Organization** to maintain the *confidentiality*, *integrity*, and *availability* of *ePHI*, by serving to limit physical access to **Organization's** electronic *information system*s and the *facility* and facilities in which they are housed, while ensuring that properly authorized *Access* is allowed.

Facility Access controls include:

- ***Contingency operations***. Contingency operations enable **Organization** to restore of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
- ***Facility security plan.*** The facility security plan works to safeguard the *facility* and the equipment therein from unauthorized physical *Access*, tampering, and theft.
- ***Access control and validation procedures.*** Access control and validation **procedures** control and validate a person's *Access* to facilities based on their role or function, including visitor control, and control of *Access* to software programs for testing and revision.
- ***Maintenance records***. **Organization** will document repairs and modifications to the physical components of a *facility* which are related to security (for example, hardware, walls, doors, and locks).

Contingency Operations :

Organization will enable *facility Access* in support of restoration of lost data under the disaster recovery plan and business continuity plan (emergency mode operations plan) in the event of an emergency.

Contingency Operations Procedure:

- **Organization** will take reasonable steps to ensure that in the event of a disaster or emergency, while operating in emergency mode, appropriate workforce members can enter its facilities to take the necessary actions as indicated in its respective procedures as set forth in the Disaster Recovery Plan and Emergency Mode Operation Plan.
- **Organization** will allow only authorized workforce members or business associates *Access* to its facilities to support restoration of lost data. The Disaster Recovery Plan will identify which individuals are allowed such access.

- **Organization** will define workforce members' roles in its Disaster Recovery Plan, and address facilities, *ePHI* Systems, and electronic media involved.
- **Organization**'s Disaster Recovery Plan should define how the actions taken by such workforce members are tracked and logged, and how unauthorized *Access*es can be detected and prevented.
- Based on the Emergency Mode Operations Plan, **Organization** will allow authorized workforce members to enter **Organization**'s facilities to enable continuation of processes and controls that protect the *confidentiality*, *integrity* and *availability* of *EPHI* while operating in emergency mode.
- **Organization** will define workforce members' roles in its Emergency Mode Operations Plan.
- **Organization** will ensure that its Emergency Mode Operations Plan defines how the actions taken by such workforce members are tracked and logged, and how unauthorized *Access*es can be detected and prevented.
- **Organization** will require that only authorized workforce members are permitted to administer or modify processes and controls that protect the security of *ePHI*. **Organization**'s Emergency Mode Operations Plan will define such workforce members and roles.

Safeguarding the *Facility* and Equipment from Unauthorized *Access*, Tampering and Theft:

Organization will safeguard the *facility* and the equipment therein from unauthorized physical *Access*, tampering, and theft. **Organization** will ensure that systems and electronic media that contain *ePHI* are located in physically secure locations. Physically secure locations are those that are not routinely *Access*ible to the public.

***Facility* Safeguard Procedures:**

Organization will limit physical *Access* to electronic information hardware and the *facility* or facilities in which they are being housed, while ensuring properly authorized *Access* is allowed:

- **Organization** will utilize *facility Access* controls. Appropriate controls may include *Access* control cards at doors, guest *Access*, burglar alarms, etc.
- **Organization** will ensure that workforce members do not share *Access* cards to enter the *facility*.
- **Organization** will ensure that workforce members do not allow other persons to enter the *facility* by "piggy-backing" *(entering the facility by walking behind an authorized person, through a door without using a card in the reader);*.
- **Organization** will prohibit employees from sharing hard key *Access*, alarm codes, or keypad codes to enter the *facility*; and
- **Organization** will require visitors to sign in and sign out, and be escorted through any common areas (excluding ingress or egress), or when in any room or area containing unsecured or visible *ePHI*.

Specific Physical Component *Security measures*:

- **Metal/Hard Keys:** Facilities that use metal/hard keys will change affected or appropriate key locks when keys are lost or a workforce member leaves without returning the key. In addition, these facilities will use a mechanism to which workforce members are provided key *Access*.
- **Network Closet(s): Organization** will ensure that every network closet is locked whenever the room is unoccupied or not in use. **Organization** will document who has *Access* to the network closets, and will update the documentation when *Access* authorization changes.
- **Server Room(s): Organization** will lock server rooms when the room is unoccupied and not in use. **Organization** will document who has *Access* to each server room, and will update the documentation when *Access* authorization changes.
- **Alarm Systems: Organization** will ensure that all facilities that have *ePHI* should have some form of alarm system that is activated during non-business hours. **Organization** will ensure that alarm system codes are only provided to workforce members that require this information in order to leave and enter a building.
- **Doors**: **Organization** will ensure that all external *facility* doors and doors to areas where *ePHI* is housed are closed at all times. Workforce members should ensure that doors being entered or exited are completely shut before leaving the vicinity. If a door closing or locking mechanism is not working, workforce members notify their immediate supervisor as soon as possible.

Procedures: Documentation

Organization will implement a maintenance schedule that specifies and documents how and when *facility* safeguard procedures will be reviewed and tested, and will implement a process for maintaining and revising these procedures.

***Access* Control and Validation Procedures:**

Organization will implement *facility Access* controls to control and validate a person's *Access* to facilities based on their role or function. **Organization** will implement visitor *Access* controls, and *Access* controls to software programs for testing and revision.
An example would be to mandate that all visitors must be escorted through any patient areas.

- **Organization** will provide workforce members *Access* rights to areas and systems containing *ePHI* only as needed in order to accomplish a legitimate business task.
- **Organization** will periodically review and, where necessary, revise *Access* rights to the facilities and *ePHI* Systems.
- **Organization** will instruct workforce members not to attempt to gain physical *Access* to facilities containing *ePHI* Systems for which they have not been given proper authorization to *Access*.
- **Organization** will require that workforce members immediately report the loss or theft of any device (e.g., card, token) that enables physical *Access* to facilities to the

Security Official. c. to carry or display an identification badge when at facilities containing *EPHI* Systems.

- **Organization** will require that visitors to a *facility* present proper identification, that visitors sign in and sign out, and that visitors provide their reasons for needed *Access* prior to gaining *Access*.
- **Organization** will periodically review termination procedures, including a review of physical key inventory or other *facility Access* measures (such as electronic door *Access*), to ensure that *Access* authorization is current.
- **Organization** will provide for control of *Access* to software programs for testing and revision *Developers seldom need Access to live data. Best practices usually mandate that data in development environments is anonymized. Developer Access is thus blocked from the ePHI storage areas of the application or server.*

Maintenance Records Procedures:

Organization will document repairs and modifications to the physical components of a *facility* which are related to security (for example, hardware, walls, doors, and locks).

- **Organization** will identify who is responsible for maintaining, recording, and securely storing maintenance and modification repair documentation
- Such documentation will be maintained in the form of a trackable log, and contain:
    - Date and time of repair or modification;
    - A description of the physical component prior to repair or modification;
    - The reason(s) for repair or modification (including any damage and any related security incident),
    - The names and titles of the person(s) performing repair or modification;
    - The outcome of the repair or modification.

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*

Security Policy 11.0 *Workstation* Use and *Workstation* Security

FULL POLICY LANGUAGE:

Policy Purpose:

This policy outlines how **Organization** will protect *ePHI* from unauthorized, incidental, or accidental *workstation* viewing or *Access*, through ***workstation* use** *Access* controls, and ***workstation* security** *Access* controls.

Policy Description:

Organization will utilize *workstation use Access* controls and *workstation* security *Access* controls. *Workstation* use controls will ensure that functions or activities performed on *workstation*s containing or *Access*ing *ePHI* are consistent with workforce members' roles. This means that *user*s may only have *Access* to that *ePHI* they need to perform their job.. W *Workstation* security *Access* controls consist of safeguards that **physically restrict** *workstation Access* to only authorized *user*s.

***Workstation* Use:**

Organization will ensure that the workforce complies with the following *workstation* use procedures:

- **Organization** will instruct employees how to adequately shield observable *ePHI* from unauthorized disclosure and unauthorized *Access* on computer screens.
- **Organization** will train employees as to where to place and position computers to only allow viewing by authorized individuals. Once trained, the workforce shall make every effort to ensure that *ePHI* and any other confidential information on computer screens is not visible to unauthorized persons. An example of proper placement and positioning: If the receptionist's screen is visible from the patient exit area, workforce members will either put a screen cover on the monitor or move the desk to minimize incidental viewing of PHI.
- Workforce members working in facilities that are not part of **Organization** will maintain awareness of their surroundings to ensure that no one can incidentally view *ePHI*, and that no *ePHI* is left unattended. Workforce members who travel to different locations during the workday to collect or to transmit *ePHI*, may not leave *ePHI* unlocked or visible in their vehicles. Devices containing *ePHI* should be locked and stored out of sight (such as in the trunk). In addition, these workforce members may not leave any *ePHI* in client facilities/homes.
- **Organization** will utilize session lock for *workstation*s. A session will lock after a maximum of 15 minutes of inactivity (best practice: 5 minutes). Session lock blocks

further *Access* until the workforce member logs back in using the identification and *authentication* process.

- Members of the workforce may not **store** *ePHI* on non-approved devices or equipment. In smaller or simple environments, this can mean prohibiting the use of any devices that are not included on the Device Audit. In order to ensure that *ePHI* is not stored on non-approved devices or equipment, **Organization** might implement zero trust or network *Access* control solutions.
- Members of the workforce may not **copy or transmit** *ePHI* onto non-approved devices or equipment. In smaller/simpler environments, this can be managed through policies, procedures, and training. In higher-risk environments, data classification and control solutions may be implemented to actually prevent the transfer of data to unapproved locations. Example: **Organization** uses Microsoft, but a receptionist prefers using Dropbox. In such a circumstance, **Organization** may not allow the receptionist to upload *ePHI* to Dropbox, unless Dropbox is **Organization**'s business associate, with a business associate agreement on file.
- **Organization** will require that remote *Access* to *ePHI* by workforce members who work from home or other non-office sites, be through secure channels only. This secure channel requirement applies to workforce members who telecommute, to workforce members who are traveling, and when workforce members are at locations other than the *facility*. **Organization**, to ensure *Access* is through secure channels, may require the use of VPN for all remote workforce members, and may implement a Remote Workforce Member Policy.
- Members of the workforce may not store unencrypted *ePHI* on portable electronic devices, including laptops.

Additional *Workstation* Use Controls:

- Any material containing PHI or *ePHI*, or material that is otherwise confidential or sensitive, must be removed from an employee's desk and locked in a drawer, when the desk is unoccupied and at the end of the work day.
- File cabinets containing PHI, or material that is otherwise confidential or sensitive, must be kept closed and locked when not in use or when not attended.
- Keys used for *Access* to PHI, or otherwise confidential or sensitive information, may not be left at an unattended desk.
- *Password*s may not be left on sticky notes posted on or under a computer, nor may *password*s be left in writing in an *Access*ible location.
- Printouts or faxes containing PHI or otherwise confidential or sensitive information should be immediately removed from the printer or fax. Printouts that are no longer needed should be shredded as soon as possible.
- Upon disposal, PHI or otherwise confidential or sensitive information must be shredded in official shredder bins or placed in locked, confidential disposal bins.
- Portable *computing devices* such as laptops/tablets must be kept in a locked drawer, cabinet, or closet.

- Portable *storage devices* such as USB drives must be kept in a locked drawer, cabinet, or closet.

***Workstation* Security Procedures:**
Organization will utilize a series of safeguards, to restrict *Access* to *workstation*s that *Access ePHI* to authorized *user*s.

Safeguards include:

- **Organization** will require that all workforce members receive permission from their supervisor before removing *ePHI* from their *facility*. Approvals shall specify the type of permission and the time period for authorization.
- **Organization** will maintain an accurate inventory of all systems with *Access* to *ePHI*.
- **Organization** will require that all laptops be stored in a secure/locked location.
- **Organization** will enforce device wipe after repeated unsuccessful login attempts.
- **Organization** will implement additional physical controls for removable media on which *ePHI* is stored. Such controls may include enabling computing devices with a *password*-protected screen saver with session lock or automatic logoff to ensure protection of computing devices when a *user* is away from the device; ensuring the device is physically secured; is encrypted if possible; and requiring that the media be in the physical possession of the *user* at all times. Removable media is easy to lose. If **Organization** has to use thumb drives or external hard drives, **Organization** should maintain
- Securing computing devices (automatic session logoff or lock) prior to leaving the device area to prevent unauthorized *Access*. Devices and applications, including those in waiting rooms, offices, and other areas, may be set to log off after a specific time of inactivity, for up to 15 minutes (best practice is five minutes).
- Exiting running applications and closing open documents after use or inactivity.

RELEVANT HIPAA REGULATIONS:

- §164.310(b) *Workstation use*
- §164.310(c) *Workstation security*

Security Policy 12.0 Device and Media Controls

FULL POLICY LANGUAGE

Policy Purpose:

This policy sets forth procedures governing the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a *facility*, as well as the movement of these items within the *facility*.

Policy Description:

This policy sets forth rules for the following:

- ***ePHI Disposal:*** **Organization** will require proper final disposal of *ePHI* and/or the hardware or electronic media on which it is stored.
- ***Media re-use controls:*** **Organization** will ensure proper removal of ePHI from electronic media before re-use of that media, through specific sanitization controls.
- ***Accountability controls:*** **Organization** will maintain a record of the movements of hardware and electronic media, and any person responsible for such movement.
- ***Data Backup and Storage:*** **Organization** will create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

General Procedures:

Organization will maintain and update an inventory of all hardware and electronic media containing *ePHI*. Each hardware and electronic media will be assigned a unique name, be stored in a locked storage area, signed out, and signed in. **Organization** will maintain a log of sign-ins and sign-outs. The inventory will be updated to make note of when electronic media and media that contain *ePHI* are moved, either into, out of, or within the *facility*.

Disposal Procedures:

Organization will instruct employees on:

- How *ePHI* is to be disposed of.
- Which employees are authorized to perform *ePHI* disposal.
- Which employees are authorized to dispose of hardware or electronic media on which *ePHI* is stored.

Proper disposal requires that the *ePHI* or electronic media on which *ePHI* is stored be rendered unusable, unreadable, and/or in*access*ible. There are three NIST-recognized media sanitization methods – clearing, purging, and destruction. **Organization** will select the appropriate sanitization method(s) for all *ePHI* disposal.

- **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** 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** 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.

Media Reuse:
Organization requires that *ePHI* on hardware and electronic media be rendered unusable and/or in*access*ible before these are made available for reuse, whether for a worker who does not require *Access* to the *ePHI*, or when the equipment is transferred to a new worker with different *ePHI Access* needs. **Organization** will ensure that hardware and electronic media will be rendered unusable and/or in*access*ible in accordance with NIST cleaning and purging standards, as applicable.

Accountability:
Organization will prepare an inventory that identifies all hardware and electronic media containing *ePHI*. **Organization** will physically confirm the contents of the inventory on at least an annual basis. **Organization** will maintain an accurate Device Inventory and review it as part of the Device Audit.

To implement the accountability control, **Organization** will also implement a tracking system. This tracking system will document the assignment of responsibility for hardware and electronic media containing *ePHI*, as well as the transfer of authority of these devices. **Organization** will maintain a record of the transfer of hardware and electronic media between its point of origination and point of receipt. **Organization** will ensure that the record includes the names of the individuals responsible for the hardware and electronic media. Examples of documentation include documenting when laptops are sent out the manufacturer for repair, or, assigning a *user* a specific computer and documenting

this on your Device Inventory. To ensure that hardware and electronic media can be accurately and appropriately tracked, **Organization** will require that loss or theft of electronic equipment or media containing *ePHI* be immediately reported to authorized personnel.

Data Backup and Storage:
Organization will require the testing of backups prior to moving any equipment inside of or outside of **Organization.** Testing measures will account for what equipment is to be tested, who performs the testing, and documentation of test results. **Organization** will then ensure that a retrievable, exact backup of *ePHI* is available before movement of equipment.

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*

Security Policy 13.0 *Access* Controls

FULL POLICY LANGUAGE

Policy Purpose:
This policy sets forth **Organization**'s rules for *Access* controls. *Access* controls are technical measures that ensure that only those persons or programs that have been granted *Access* rights to *ePHI* are allowed such *Access*.

Policy Description:
Organization must safeguard the *confidentiality*, *integrity*, and *availability* of electronic protected health information. To do this, **Organization** will implement policies and procedures that reasonably and appropriately restrict *Access* to only those persons and entities with a need for *Access*. These procedures are called *Access* controls.

Organization will implement *Access* controls that are appropriate for the role of each workforce member. **Organization** will implement *Access* controls that grant authorized *user*s the rights and privileges to *Access* the minimum necessary information to perform their jobs, and no more.

Organization will provide rules for and will implement the following *Access* controls:

1. Unique *User* Identification
2. Emergency *Access* Procedure
3. Automatic Logoff
4. *Encryption* and Decryption

Unique *User* Identification:

Unique *user*names/*user* IDs and *password*s play an important role in protecting the *confidentiality*, *integrity*, and *availability* of *ePHI*. Unique *user*names/*user* IDs and *password*s allow system processes to identify the *user* and associate the *user* with actions taken by or on behalf of that *user*. Unique *user*names/*user* IDs and *password*s allow for recording of a *user*'s actions to audit logs, which can be reviewed for inappropriate *Access* to *ePHI* and traced back to a specific workforce member.

Unique *User* Identification Procedures:

- **Organization** will assign each *user* with a unique *user*name/*user* ID and *password* for *Access* to *ePHI*. This will enable **Organization** to identify and track *user* identity and actions.
- **While Organization** will permit the use of shared mailboxes in certain instances, **Organization** will not allow sharing of credentials.
- **Organization** may share a mailbox to multiple *user*s, but multiple *user*s may not share a single logon to any account with *Access* to *ePHI*.
- In a few specific circumstances, **Organization** may permit shared email addresses. **Organization** may choose to use a shared email address for establishing an office or division for the receipt of complaints. If **Organization** requires shared mailboxes, **Organization** will implement a policy and procedure for acceptable use.

Emergency *Access* Procedure:
Organization will establish policies and procedures to ensure that necessary *ePHI* may be *Access*ed during an emergency. These policies and procedures will identify roles that may require special *Access* to *ePHI* during an emergency.

Granting *Access* in an Emergency: Emergency *User Access*
Organization may, in an emergency, grant emergency *Access* to *ePHI* to those workforce members who have not completed security training, or whose job roles do not ordinarily require *Access*, under the following circumstances:

- **Organization** declares an emergency or is responding to a natural disaster, that makes the management of client information security subordinate to immediate workforce safety concerns and activities.

- The normal methods for obtaining *Access* have failed due to a crisis situation.
- **Organization** determines that granting immediate *Access* is in the best interest of a patient whose *ePHI* may be exposed if such *Access* were not granted.

When emergency *Access* is granted, **Organization** will document the *Access* determination and the reasons for granting the *Access*. The Security Official will review the emergency *Access* to determine whether it should remain in effect. When the Security Official determines that the emergency *Access* is no longer necessary, the Security Official will terminate the emergency *Access*.

Granting Emergency *Access*: Granting *Access* to an Existing *User Access* Account:
In some circumstances, **Organization**'s management may need to grant itself emergency *Access* to a *user*'s account, without the *user*'s knowledge or permission. Management, with the approval of the Security Official, may grant this emergency *Access* in these situations:

- The workforce member is terminated or resigns, and management requires *Access* to the person's data;
- The workforce member is on approved leave of absence for a prolonged period;
- The workforce member has not been in attendance and therefore is assumed to have resigned, as per what constitutes "resignation" under **Organization**'s employment handbook or similar policy; or
- The workforce member's superior needs immediate *Access* to data on a workforce member's computer to provide client treatment.

Session Lock:
Organization will implement electronic procedures that lock an electronic session after a predetermined time of inactivity (no longer than 15 minutes; best practice is 5 minutes).

Different *information system*s do not necessarily require the same period of inactivity before `session lock` is implemented. For example, a risk assessment might determine that the data in one *information system* is sensitive, and set the `session lock` to occur after five minutes of inactivity, while the data in a different system is not sensitive and `session lock` period could be set for ten minutes.

***Encryption* and Decryption:**
Organization will implement *encryption* and decryption measures to protect *ePHI* from unauthorize *Access*. These measures will serve to prevent the storage of unencrypted *ePHI* on portable electronic devices, including laptops.

In some instances, *encryption* for stored *ePHI* is genuinely not feasible, or it is impossible. In such instances, **Organization** will adopt alternative, reasonable, and appropriate compensating controls, including:

- Unique ID and *password authentication* and *user* profiles.
- Physical *security measures* for facilities and *workstation*s, including appropriate device and media controls.
- System security auditing and logging.
- Monitoring of audit reports and logs.
- Correct configurations of applications to use secure protocols.
- Automatic logoff and/or screen lock.
- Secure remote *Access*.
- Correctly configured firewalls.

RELEVANT HIPAA REGULATIONS:

- 164.312(a)(1) *Access control*

Security Policy 14.0 Audit Controls

FULL POLICY LANGUAGE

Policy Purpose:

Organization will establish a mechanism for audit log creation, examination of the activity in audit logs, and audit log retention.

Policy Description:

This policy sets forth criteria for implementing hardware, software, and/or procedural mechanisms that will record and examine *information system*s activity. These mechanisms are known as audit logs.

Audit Log Procedures:

Log Files Creation: For each *information system*, **Organization** will implement audit logging for the purposes of detecting *security incidents* including wrongful *Access*, disclosure, and data modification.

Log Files Content: Organization will record sufficient *user* and system information to establish when someone has created, *Access*ed, modified, or deleted *ePHI*. **Organization** will ensure that the audit record captures sufficient information to establish what events occurred, the sources, and the outcomes of the events.

Log files should include, at a minimum:

- Type of event and result.

- Time and day the event occurred.
- *User* ID associated with the event.
- Program or command used to initiate the event.

Log File Examination:
The Security Official will review audit logs, activity reports, or other mechanisms to document and manage system activity. The Security Official will report indications of improper use to management for investigation and follow-up.

Log Files Retention:
Organization will retain log files, at a minimum, until an *information system* activity review (164.308(a)(1)(ii)(D) of the files is performed and documented as outlined in the Security Management Process Policy (Security 2.0). The Security Official will determine what additional retention period may be necessary beyond the completion of a system activity review in order to meet operational, risk management, or regulatory requirements.

Log Files Security:
Unauthorized *Access* to, modification or deletion and other falsification of log files are strictly prohibited. Audit information and audit tools shall be protected from unauthorized *Access*, modification, and deletion. *Security measures* include:

- ***Access* Restrictions. Organization** will restrict *Access* to an *information system*'s log files to only that system's System Owners, System Administrators, and other persons responsible for performing system activity review and incident handling.
- **Separation of Duties.** Whenever possible, **Organization** security personnel who administer the *Access* control function will not also administer the log files.

Log Files Back-up and Storage Requirements:
Organization will ensure that audit logs of *Access* to *information system*s, devices, and equipment containing PHI are backed up, documented, and archived.

RELEVANT HIPAA REGULATIONS:

- §164.312(b) *Audit controls*

Security Policy 15.0 *Integrity* Controls

FULL POLICY LANGUAGE

Policy Purpose:

To set forth **Organization's** procedures to protect *ePHI* from alteration or destruction in an unauthorized manner.

Policy Description:

Organization will implement policies and procedures to protect *ePHI* from unauthorized alteration, destruction, or disclosure by implementing a series of *integrity* controls. These controls consist of *authentication* measures and data and system *integrity* checks.
Organization will also implement mechanisms to **corroborate** that *ePHI* has not been altered, destroyed, or disclosed in an unauthorized manner.
Methods to protect *ePHI* from unauthorized alteration, destruction, or disclosure will include:

- **Electronic *Authentication***. **Organization** will implement electronic mechanisms (e.g., error-correcting memory, digital signatures, checksum technology) when such mechanisms are available, employable and commensurate with the criticality and risks associated with the *ePHI*.
- **Procedural *Authentication***. If electronic *authentication* mechanisms are not available or employable, or in order to augment electronic mechanisms, **Organization** will implement procedural mechanisms (e.g., manual data validation) when such mechanisms are appropriate, based on the criticality and risks associated with the *ePHI*.
- **Data and System *Integrity* Checks**. **Organization** will establish 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). The frequency of data and system *integrity* checks will be commensurate with the criticality and risks associated with the *ePHI*, but no less than on an annual basis.
- ***User* Reporting. Organization** will require *user*s to report suspected vulnerabilities or unauthorized *ePHI* data modification or destruction to the Security Official.

Organization will also implement electronic mechanisms **to corroborate** that electronic protected health information has not been altered or destroyed in an unauthorized manner.

These mechanisms must be capable of detecting (1) whether *ePHI* has been altered or destroyed; and (2) If so, whether the alteration or destruction is unauthorized.

Organization will implement the following mechanisms to corroborate that *ePHI* has not been altered or destroyed in an unauthorized manner:

- **Organization** will implement running alerts for unusual logon and *Access* length and times.

- **Organization** will protect sensitive data with appropriate measures, such as *malicious software* protection, secure file standards, and use of web browser security standards.
- **Organization** will implement processes to notify *user*s, and take other appropriate remedial action, in the event that *malicious software* has been propagated

RELEVANT HIPAA REGULATIONS:

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

Security Policy 16.0 Person or Entity *Authentication*

FULL POLICY LANGUAGE

Policy Purpose:

Organization will implement procedures to verify the identity of a *user*, process, or device, so as to allow *Access* to electronic *information system*s. These procedures are known as *authentication* procedures.

Policy Description:

Organization will use a series of measures to authenticate that an individual or entity seeking *Access* to *ePHI* is in fact the person or entity whom they claim to be:

- **Organization** will implement a procedure to provide each *user* with a unique account, with a unique *user*name and strong *password*, to verify that a person or entity seeking *Access* is the one claimed. Two-factor *authentication* or multi-factor *authentication* may also be used to verify identity. Biometric *Access* measures may also be used for verification purposes.
- **Organization** will regularly review, as appropriate, all *workstation*, operating system, and application logs, as well as failed or successful challenges to account permissions.
- **Organization** will implement procedures to ensure that systems and applications are not configured to save *password*s. *Password* files on authenticating servers will be adequately protected and encrypted.

***Authentication* Procedures:**

Organization *authentication* processes include:

- Documented procedures for granting persons and entities *authentication* credentials or for changing an existing *authentication* method.

- Documented procedures for detecting and responding to any person or entity attempting to *Access ePHI* without proper *authentication*.
- Removing or disabling *authentication* credentials in *ePHI* systems for persons or entities that no longer require *Access* to *ePHI*.
- Periodic validation that no redundant *authentication* credentials have been issued or are in use.
- When feasible, masking, suppressing, or otherwise obscuring the *password*s and PINs of persons and entities seeking to *Access ePHI* so that unauthorized persons are not able to observe them
- **Organization** will limit *authentication* attempts.
    - *Authentication* attempts that exceed the limit may result, as appropriate, in:
        - Disabling relevant account for an appropriate period of time.
        - Logging of event.
        - Notifying appropriate **Organization** management..

RELEVANT HIPAA REGULATIONS:

- 164.312(d) *Standard: Person or Entity Authentication*

Security Policy 17.0 Transmission Security

FULL POLICY LANGUAGE

Policy Purpose:

This policy describes **Organization**'s transmission security procedures, which are mechanisms to guard against unauthorized *Access* to *ePHI* being transmitted over an electronic communications network.

Policy Description:

Organization will implement reasonable and appropriate measures to guard against unauthorized *Access* to and protect the *integrity* and *confidentiality* of *ePHI* that is transmitted over an electronic communications network. Such measures will ensure *ePHI* has not been modified without authorization, or corrupted, without detection during transmission.

Measures to Ensure *ePHI* is Not Improperly Modified Without Detection Until Disposed of:

- **Organization** will ensure that wired and wireless transmission of *ePHI* will utilize secure protocols (*encryption*).
- **Organization** will require that all remote *Access* to *ePHI* be by secure means only.
- **Organization** will prohibit sending of unprotected *ePHI* by unencrypted email, UNLESS medical records containing the *ePHI* have been requested by a patient who

specifically requires them to be delivered in an unencrypted email. The best practice here is to warn the patient that this is not a secure method of communication, and to obtain the patient's acknowledgment and consent) in writing, prior to sending.
- **Organization** will consider the mandating of Virtual Private Network (VPN) for all remote *user*s.
- **Organization** will ensure that employees delete or redact *ePHI* from the body of received email before replying to it.

Organization will implement a mechanism to encrypt *ePHI* whenever deemed appropriate.

Procedures:

- **Organization** will implement *encryption* measures to encrypt data at rest.
- **Organization** will implement *encryption* measures to encrypt data in motion.
- **Organization** will implement *encryption* measures for files, data, and devices containing *ePHI*.
- **Organization** will implement end-to-end *encryption* for external emails containing *ePHI*.
- **Organization** will implement a mechanism to encrypt electronic protected health information in any other situations whenever it is deemed appropriate. In such situations, data at rest and data in motion should be encrypted. Full disc *encryption* should be implemented. Files, data, and devices containing *ePHI* should be encrypted. Email *encryption* should be end-to-end.

RELEVANT HIPAA REGULATIONS:

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

Security Policy 18.0 ePHI Safeguards

FULL POLICY LANGUAGE:

Policy Purpose:

It is the policy of **Organization** to ensure that *ePHI* is protected from misuse, loss, tampering, or use by unauthorized persons. This policy addresses the safeguarding of *ePHI* received, created, used, maintained, and/or transmitted via the communication media listed. *ePHI* shall be disclosed to personnel, patients, their personal representatives, other covered entities, public health officials, and business associates, in accordance with HIPAA regulations and this policy.

Policy Description:

The HIPAA Privacy Rule, 45 CFR 164.530, requires **Organization** to develop and implement safeguards to protect the privacy of PHI and *ePHI*. The HIPAA Security Rule section 164.306(a) requires the safeguarding of the *confidentiality*, *integrity*, and *availability* of *ePHI* that **Organization** creates, receives, maintains, or transmits. Together, these two rules provide safeguards for communication of *ePHI*.

Procedures:

Emailing *ePHI*:

Organization should take certain precautions when using email to avoid unintentional or unauthorized disclosures. These include:

1. Checking the email address for accuracy before sending, and sending an email alert to the patient for address confirmation prior to sending the message.
2. Encrypting treatment-related communications.
3. Limit the PHI contained in the email to the minimum necessary to accomplish the purpose of the communication.
4. Email PHI only to a known party (i.e., patient, health care provider).
5. Prior to emailing encrypted PHI to an individual:
   - Obtain the individual's consent to communicate *ePHI* with him or her even if the individual initiated the correspondence; and
   - Clearly communicate to the individual the risks and limitations associated with using email for communications of *ePHI*.

   1. Before emailing to a non-healthcare provider third party, obtain the consent of the individual who is the subject of the *ePHI*.
   1. Do not email *ePHI* to a group distribution list unless all individuals have consented to such a method of communication.
   1. In the subject heading, do not use patient names, identifiers or other specifics; consider the use of a *confidentiality* banner such as "This is a confidential medical communication."
   1. Include in the email a *confidentiality* notice, such as the following: "*Confidentiality* Notice: This email transmission, and any documents, files or previous email messages attached to it, may contain confidential information. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution, or use of any of the information contained in or attached to this message is STRICTLY PROHIBITED. If you have received this transmission in error, please immediately notify us by replying to the email or by telephone at (XXX) XXX-XXXX, and destroy the original transmission and its attachments without reading or saving them to disk."

Patients may request that **Organization** send patients **unencrypted** email messages, email attachments, or texts that contain *ePHI*. If they do, **Organization** must comply with the request, but only after warning of risks involved and obtaining written consent.

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*

Security Policy 19.0 Policies and Procedures

FULL POLICY LANGUAGE:

Policy Purpose:

This policy describes what ongoing measures **Organization** shall take to comply with the standards, implementation specifications, and other requirements of the HIPAA Security Rule.

Policy Description:

This policy describes the measures **Organization** must implement to comply with the Security Rule, along with who is responsible for implementing the measures, how and when the measures will be documented and who is entitled to *Access* to documentation pertaining to this compliance.

Procedures:

1. The Security Official will implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rule.
2. All policies and procedures implemented to comply with the HIPAA Security Rule shall be documented in writing (which may be in electronic form).
3. All records of actions, activities, or assessments required to be taken or performed by the Rule shall be documented. The documentation shall be detailed enough to communicate the *security measures* taken and to facilitate periodic evaluations.
4. This Documentation shall be retained for a minimum of six (6) years from the time of its creation or the date when it last was in effect, whichever is later.
5. **Organization** will make all documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
6. Documentation shall be reviewed at least annually, and updated as needed, in response to environmental or operational changes affecting the security of the *ePHI*.

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*

Security Policy 20.0 HIPAA Incident Response and Reporting and Breach Determination

FULL POLICY LANGUAGE:

Policy Purpose:

Organization takes the privacy, security and *integrity* of *individual*'s data seriously. **Organization** also has legal responsibilities to protect *PHI* under *HIPAA*, to identify and respond to suspected incidents, require its *workforce members* to report incidents, and to determine when there is a reportable *breach* of an *individual*'s *PHI*.

The purpose of this Incident Response and Reporting and *Breach* Determination Policy is to meet **Organization's** responsibilities and to provide guidance to **Organization** *workforce members* regarding recognizing and reporting a privacy or *security incident* involving Member health information. **Organization** will review all reported incidents and will follow the procedures set forth to determine if there has been a *Breach* (an acquisition, *Access*, use, or disclosure of the Member's *unsecured PHI* in a manner not permitted under *HIPAA*).

Policy Description:

This policy establishes guidelines for **Organization** to

- Require the reporting of suspected privacy and *security incidents* (any attempted or successful unpermitted or unauthorized *Access*, use, disclosure, modification, interference or destruction of *unsecured PHI* in any form). The HIPAA Security Rule defines a "security incident" as the attempted or successful unauthorized *Access*, use, disclosure, modification, or destruction of information or interference with system operations in an *information system*. All *workforce members* must report any suspected incident to the Compliance, Privacy or Security Official as soon as possible, and may report anonymously through The Guard if preferred. *Workforce members* who fail to promptly report incidents will be subject to discipline.
- identify and respond to suspected or known incidents involving the security or privacy of protected health information, including mitigating any harmful

effects. **Organization** will handle any complaint that is potentially a privacy or *security incident* under this Policy, which also appears in the Security Manual, instead of Privacy Policy 5.0: *Complaints to the* ***Organization***.
- determine if there has been a *Breach* of *unsecured PHI* ("*PHI*") after analyzing potential exceptions and performing a risk analysis or requiring any involved *Business associate* to do so and then reviewing their determination, and
- document the incidents, responses and *Breach* determinations and retain the documentation for at least six years.

Procedures:

Reporting of *Security incidents*:

Organization will train all *workforce* Members on *HIPAA* privacy and security requirements. All **Organization** *workforce members* must report to their supervisor and/or **Organization's** Compliance, *Privacy Official* or Security Official as soon as possible and in no event later than 24 hours after discovering any suspected, known, or potential Privacy or *Security incident*. Supervisors must notify the Privacy and Security Officials immediately upon notification of potential, known or suspected Incidents. **Organization** *workforce members* are subject to discipline for failure to promptly report any suspected, known, or potential *Breach* of *unsecured PHI*.

Organization will require *Business associates* to report Privacy and *Security incidents* promptly and will enforce contract requirements.

Monitoring for Privacy and *Security incidents*:

Organization shall employ tools and techniques to monitor events, detect attacks and provide identification of unauthorized use of the systems that contain Electronic Protected Health Information (*ePHI*) and also periodically review *Access*, *integrity*, use and disclosure of all *PHI*, in whatever form, to identify any potential *breach*es.

Treatment of Recurring and Expected Unsuccessful *Security incidents*.

Organization acknowledges the ongoing existence or occurrence of attempted but "Unsuccessful *Security incidents*" including but not limited to, pings, and other broadcast attacks on firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above. As long as no such Unsuccessful *Security incident* results in unauthorized *Access*, use or disclosure, inappropriate denial of *Access* or harm to the *integrity* of *ePHI*, they will be reviewed, and the reports kept but **Organization** will not undertake a full factual investigation or *breach* determination analysis for each such unsuccessful attempt. Unsuccessful *Security incidents* will also be reviewed for heightened frequency and considered in the development, implementation of and improvements to safeguards. **Organization** will perform a thorough analysis of any suspicious circumstances or unusual activity found during reviews.

Perform and Document a Factual Investigation of the Incident

Organization will perform a factual investigation of any reported potential privacy or *security incident*. At a minimum, **Organization** will seek information and documentation sufficient to a) perform an analysis of whether there was any attempted or successful *unauthorized Access*, use, disclosure, modification, or destruction of information in any form, b) determine if any unsecured information was involved, c) determine if any *PHI* was involved d) determine if any exception to an assumption of a *Breach* of *PHI* exists, e) perform the risk of *PHI* compromise analysis and f) determine the number of *individual*s impacted. If **Organization** has a separate investigations policy, it will follow that policy. **Organization** may retain outside resources for the completion of some or all of the investigation, especially if a forensic investigation is desirable.
Should the Privacy or *Security incident* occur through a *Business associate*, **Organization** may rely on the *Business associate* to conduct an investigation but may also conduct an independent investigation if it so chooses. **Organization** must review the *Business associate's* findings and underlying facts prior to deciding on whether or not to rely solely on the *Business associates* investigation or to perform its own investigation.

Determine if There Was Any Attempted or Successful Unauthorized *Access*, Use, Disclosure, Modification, or Destruction of Information in Any Form
Following a standard procedure and utilizing the *HIPAA Breach* Risk Assessment Record and *Unsecured PHI* Job Aid or similar documentation when applicable, **Organization** will determine whether a) there was any attempted or successful *Access*, use, disclosure, modification or destruction of information, b) whether the information involved was unsecured, c) whether such information was *PHI* or *ePHI*, d) whether such *Access*, use, disclosure, modification, or destruction was unauthorized or unpermitted and e) whether any exceptions to a determination of a *breach* is applicable.
Organization will use the *Unsecured PHI* Job Aid or a similar standard assessment tool to determine if any information involved in the incident was unsecured.

Organization will determine if the information involved in the attempted or successful unauthorized *Access*, use, disclosure, modification, or destruction of information was *PHI*. For example if the information involved a deceased *individual*, **Organization** will determine if the *individual* been deceased for more than fifty years.

Organization will determine if *Access*, use, disclosure, modification, or destruction was unauthorized or unpermitted by determining if the use or disclosure was authorized or permitted under *HIPAA*. For example, **Organization** will determine if it was authorized by the *individual*, required by law, or permitted as incidental.

20906 Determine if there is an Applicable Exception to a *Breach* Determination
As part of its *breach* determination, **Organization** will refer to the three exceptions listed in paragraph 1 of the definition of *Breach* published in 45 CFR § 164.402 to analyze whether an exception applies for the fact pattern of the Privacy or *Security incident*. **Organization** will determine and record its determination as to whether or not any of these three exceptions applies to the incident:

(i) Any unintentional acquisition, *Access*, or use of protected health information by a *workforce member* or person acting under the authority of a *covered entity* or a *business associate*, if such acquisition, *Access*, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part (Sets forth allowable uses of *PHI*). Example, when someone at a *Business associate* was looking for a record they needed to perform their responsibility and inadvertently *Access*ed Mary B's record instead of Mary A's record and did not further disclose information from Mary B's record, this exception applies.

(ii) Any inadvertent disclosure by a person who is authorized to *Access* protected health information at a *covered entity* or *business associate* to another person authorized to *Access* protected health information at the same *covered entity* or *business associate*, or organized health care arrangement in which the *covered entity* participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part (Part E sets forth allowable uses of *PHI*). Example, Dr. Brown requested an *individual*'s record to perform his job responsibilities, but Mary delivered the record to Dr. Black instead. So long as all of them work at the same CE, BA or within an organized health care arrangement and Dr. Black did not further disclose the information, there is no *breach*.

(iii) A disclosure of protected health information where a *covered entity* or *business associate* has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. Example, a nurse hands the wrong discharge papers to a patient and notices the error right away, taking back the papers.

If an exception applies, **Organization** will record its findings in the incident record and the incident can be closed. If no exception applies, there is a presumption that a *breach* has occurred. **Organization** may either perform a risk analysis according to the procedure set forth below or forego performing that analysis and follow the process for notifications under Privacy Policy 7.0: *Breach Notification*.

Perform an Analysis of Risk of Compromise to *unsecured PHI* utilizing the Four Required Factors and Other Pertinent Information

If **Organization** has determined that there is a presumption of a *breach*, **Organization** may perform a risk of compromise assessment using at least the following four required factors to determine if there is a low probability that *PHI* has been compromised that rebuts the presumption of a *breach*:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

2. The unauthorized person who used the protected health information or to whom the disclosure was made;

3. Whether the protected health information was actually acquired or viewed; and

4. The extent to which the risk to the protected health information has been mitigated.

Organization may also consider other factors in its analysis that might support a finding of a low probability of risk including but not limited to the time the information may have been *Access*ible or *Access*ed, the likelihood the information was *Access*ed, whether any complaints were received, how difficult or likely *Access* was even if there was *Access*ibility and any professional or legal requirements applicable to the person who received the information (does a legal privilege apply, was the person who received the information in healthcare and trained on *HIPAA* privacy requirements). The *HIPAA* Incident Assessment Tool may be useful in completing and documenting the risk of compromise assessment.

If the *Breach* occurred through a *Business associate*, **Organization** may rely on a *Business associate* to perform the risk of compromise assessment but must review the findings and underlying facts prior to deciding on whether or not to perform its own assessment.

Record Keeping
Organization will create and maintain a *HIPAA* incident log for all reported incidents, regardless of whether they are determined to be *Breach*es. **Organization** shall review this log periodically to determine areas that may require additional training. **Organization** will keep records concerning all reports of security or privacy incidents, any finding of an exception to the *Breach* definition, all analyses of risk of compromise to *unsecured PHI*, and the factual investigations and documentation supporting the analysis and findings. These records will be kept for a minimum of six years following the conclusion of the *Breach* determination for the incident(s). Where **Organization** has found an applicable exception to a *Breach* or made a finding of a low probability of compromise to *PHI*, **Organization's** records must sufficiently demonstrate the application of any exception or support a finding that there is a low probability of compromise to the *PHI*.

Enforcement and Reporting
Organization's Compliance Official and **Organization's** *HIPAA* Privacy and Security Officials or their designees, along with human resources, are responsible for managing, updating, and enforcing this policy. Violations of this policy must be immediately reported.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.308(a)(6)(i) *Security Incident Procedures*
45 CFR 164.308(a)(6)(ii) *Implementation Specification: Response and Reporting (Required)*
45 CFR 164.530(a)(c)(e)(f) *Administrative Requirements: Personnel Designations, Safeguards, Sanctions and Documentation, Mitigation*
45 CFR 402 *Definitions: Breach*

Security 21.0 Breach Notification

FULL POLICY LANGUAGE:

Policy Purpose:

Organization takes the privacy and *integrity* of *individual*'s personal health information seriously. **Organization** also has legal responsibilities to protect *PHI* under *HIPAA*, to determine when there is a reportable *breach* of an *individual*'s *PHI* and to make appropriate and timely notifications following a *breach*.

The purpose of this *Breach* Notification Policy is to meet **Organization**'s responsibilities and to provide guidance to **Organization** *workforce members* regarding making required notifications when a *Breach* determination has been made under Privacy Policy 7.0: *Breach Determination*.

This policy establishes guidelines for **Organization** to

- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate notifications to *individual*s impacted by a *Breach*,
- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate notifications to federal and state authorities if required by the details of the *Breach* determination,
- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate notifications to media if the findings of the *Breach* determination require them;
- Determine when and if appropriate substitute notice is allowed and to use that substitute notice when appropriate; and
- Document compliance with the requirements of *Breach* notifications.

Policy Description:

This policy establishes guidelines for **Organization** to:

- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate timely notifications to *individual*s impacted by a *Breach*;
- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate timely notifications to federal and state authorities if required by the details of the *Breach* determination including reporting of *breach*es involving less than 500 *Individuals* in a single state or geographic region to *HHS* electronically on an annual basis by March 1 (or February 29th in a Leap year) of the year following the *Breach*;
- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate timely notifications to media if the findings of the *Breach* determination require them;

- Determine when and if appropriate substitute notice is allowed and to use that substitute notice if required or desired;
- Ascertain and meet any more stringent applicable contractual notification requirements; and
- Document compliance with the requirements of this policy.

Following the determination of a *breach* under Privacy Policy 9: *HIPAA incident Reporting and Response and Breach Determination* **Organization** will determine what external notifications are required or should be made (i.e., Secretary of Department of Health & Human Services (*HHS*), media outlets, law enforcement officials, etc.), develop appropriate content for the notices, reports and postings, and communicate each notification, report or positing according to the procedures and requirements set forth below.

Procedures

Privacy and Security Officials Shall Direct all Notifications but may appropriately Delegate Activities

With input from the Compliance Official and others at their discretion, **Organization**'s Privacy and Security Officials will direct all activities required under this policy including the wording of any *Individual* Notices, *HHS* filings, communications required by contract, Media notices, and scripts (including escalation processes) for any telephone inquiries. Legal representation will be utilized if desired by the Privacy or Security Official or at the direction of anyone on the senior leadership team of the **Organization**. The Privacy and Security Official may delegate responsibilities as appropriate but remain responsible for the implementation of *Breach* Notification Policy requirements. This delegation includes allowing either another responsible *Covered entity* or a responsible *Business associate* to make the notifications. **Organization** remains responsible for assuring all requirements have been met by the delegated entity or *individual*. For responsibilities of *Business associates*, please refer to Privacy Policy 9.0: *Business associates* for more information.

Organization will Determine Notification Requirements based on the findings of the *Breach* Incident Investigation

Organization will use the Number of *Individual*s Involved to Determine Appropriate Notifications and Timing.

Individual Notification: If the number of *individual*s impacted by a *breach* is known to be less than 500, **Organization** will follow the notification Procedures set forth below for the timing and content of *Individual* Notification and Notification to *HHS*.

500 or More: If the number of *individual*s affected by the *Breach* is known to be 500 residents of a State or jurisdiction, **Organization** will provide notification to Prominent media outlets serving the State and regional area where the impacted *individual*s reside and follow the notification Procedures set forth below for the timing and content of Media Notice, *HHS* and Notification for *Breach*es Affecting more than 500 *Individual*s.

If the number of *individuals* is uncertain, **Organization** must use reasonable efforts to estimate the number of affected *individuals* and document its methods. **Organization** shall use this estimate to determine the number of *individuals* affected for determining appropriate notification procedures. Should further information or investigation prove the estimate to be incorrect, **Organization** must update any previous notifications or reports made using that estimate if the method or content of the Notice is materially different due to the change.

See Chart below for Summary of Requirements. Details of Appropriate Notice, Timing, Content and Means appear below the summary chart.

IF	Notification To	Timing*	Content	Means of Notice
Number of *Individuals* impacted is less than 500	Each person *individually*	Without unreasonable delay and in no case later than 60 days following discovery of *breach*	In plain language A. A brief *breach* description, including date and the date of B. types of *unsecured PHI* that were involved C. steps the *individual* should take to protect themselves D. what the **Organization** is doing to investigate, mitigate harm to *individuals*, and to protect against further *Breaches*; and E. Contact procedures	In writing by first class mail or by email if the affected *individual* has consented to such notice. Additional notice in urgent situations, it may do so by telephone or other means in addition to the written notice Substitute notice**
	HHS	no later than 60 days after the end of the calendar year in which the *Breaches* were discovered (March 1 or February 29th in a leap year).	In addition to content required for *individual* notice, Information Required on Current *HHS* report includes Entity Contact, BA Contact if Occurred at BA, Number of *individuals* impacted, safeguards placed prior to *breach*, mitigation efforts, safeguards placed after *breach*, number of *individuals* impacted	Completion of online form on the *HHS* website

Number of *Individual*s Impacted is greater than 500 in any State or jurisdiction	Prominent Media Outlet serving the areas where impacted *individual*s reside	without unreasonable delay and in no case later than 60 days following the discovery of a *Breach*	In plain language: A. A brief *breach* description, including date and the date of B. types of *unsecured PHI* that were involved C. steps the *individual* should take to protect themselves D. what the **Organization** is doing to investigate, mitigate harm to *individual*s, and to protect against further *Breach*es; and E. Contact procedures	Contact media and provide information to be included in publication
	HHS	without unreasonable delay and in no case later than 60 days following the discovery of a *Breach*	In addition to content required for media notice, Information Required on Current *HHS* report includes Entity Contact, BA Contact if Occurred at BA, Number of *individual*s impacted, safeguards placed prior to *breach*, mitigation efforts, safeguards placed after *breach*, number of *individual*s impacted	Completion of online form on the *HHS* website

*Subject to Law Enforcement requests for delay
**Substitute notice may be used in some situations for *Individual*s, see policy for details.

Timing

Organization will provide *Individual* notice without unreasonable delay and in no case later than 60 days following the discovery of a *Breach*. The **Organization** may also provide additional notice in urgent situations because of possible imminent misuse of the *PHI*.

Organization will provide Media Notice, when required, without unreasonable delay and in no case later than 60 days following the discovery of a *Breach*.

Organization will provide *HHS* notice by completing a web report form on the following timeline: If 500 or more *individual* residents of a State or jurisdiction are affected, **Organization** will complete the *HHS* notification without unreasonable delay and in no case later than 60 days following the discovery of a *Breach*. If fewer than 500 *individual*s are affected, **Organization** will notify *HHS* of each *Breach* no later than 60 days after the

end of the calendar year in which the *Breach*es were discovered (March 1 or February 29th in a leap year).

Discovery of *Breach*:
A *breach* of *PHI* shall be treated as "discovered" as of the first day the *breach* is known to the **Organization**, or, by exercising reasonable diligence would have been known to the **Organization** (includes *breach*es by **Organization's** *Business associates*). The **Organization** shall be deemed to have knowledge of a *breach* if such *breach* is known or if by exercising reasonable diligence would have been known, to any person, other than the person committing the *breach*, who is a *workforce member* or an *agent* of the **Organization** (i.e., a *Business associate* acting as an *agent* of the **Organization**).

Delays in timing permitted: Law Enforcement Delay
When **Organization** is notified by a law enforcement official that a notification, notice or posting required for a *Breach* would either impede a criminal investigation or damage national security, **Organization** may delay the notification, notice or posting for a) a period of time specified by the law enforcement official in writing or b) for the requested amount of time not to exceed 30 days from the date of an oral request for delay from a law enforcement official. **Organization** will extend the original 30 day delay imposed by an oral request if a law enforcement official makes a later request in writing prior to the expiration of the initial delay request. Any such oral or written request must be documented by **Organization** and the record preserved.
Workforce members should also refer to Privacy Policy 4:*Verification of Identity and Authority* when processing any law enforcement request for delay.

Content and Means of Notifications and Postings
At a minimum the content of reports, notifications and notices required by law for *breach*es of the privacy or security of *PHI* in any form must include the information set forth below and must be communicated by the means indicated:
Individual Notice: Means of Communication

In writing by first class mail or by email if the affected *individual* has consented to such notice. Utilize the **Sample *Breach* Notification format** attached to this Policy for all *Individual* Notice. If the **Organization** desires to send additional notice in urgent situations, it may do so by telephone or other means in addition to the written notice but not as a substitute for it.

Substitute *Individual* Notice
When **Organization** has insufficient contact information for ten or greater affected *individual*s, **Organization** will give notice by posting notice for 90 days on the company website or by publication in major print or broadcast media in the area where the affected *individual*s likely reside.

When **Organization** has insufficient contact information for fewer than ten affected

*individual*s it may give notice to those *individual*s by alternative written notice, by telephone or other reasonable means.

Individual Notice: Content

A. A brief description of what happened, including the date of the *Breach* and the date of the discovery of the *Breach*, if known;

B. A description of the types of *unsecured PHI* that were involved in the *Breach* (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

C. Any steps the *individual* should take to protect themselves from potential harm resulting from the *Breach*;

D. A brief description of what the **Organization** is doing to investigate the *Breach*, to mitigate harm to *individual*s, and to protect against further *Breach*es; and

E. Contact procedures for *individual*s to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

Media Notice Means of Communication and Content

For Media Notices the following information should be included and the Notice must include enough information for an *individual* to determine whether their information may have been disclosed, what they should do if it was and who to contact for more information:

A. A brief description of what happened, including the date of the *Breach* and the date of the discovery of the *Breach*, if known;

B. A description of the types of *unsecured PHI* that were involved in the *Breach* (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

C. Any steps the *individual* should take to protect themselves from potential harm resulting from the *Breach*;

D. A brief description of what the **Organization** is doing to investigate the *Breach*, to mitigate harm to *individual*s, and to protect against further *Breach*es; and

E. Contact procedures for *individual*s to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

Means of Notifying *HHS*

For a *Breach* Affecting 500 or More *individual*s **Organization** will timely complete a Notice utilizing the form on the *HHS* website (https://*OCR*portal.hhs.gov/*OCR*/*breach*/wizard_*breach*.jsf?faces-redirect=true).
For a *Breach* Affecting less than 500 *Individual*s **Organization** will timely file (within 60 days of the end of the calendar year in which the *Breach occurred*) a Notice utilizing the form on the *HHS* website (https://*OCR*portal.hhs.gov/*OCR*/*breach*/wizard_*breach*.jsf?faces-redirect=true).

Reliance on Others to Provide Notification.
Organization will determine any contractual obligations related to the *PHI*. If allowable, **Organization** may choose to rely upon notifications given by a *Business associate* for the *Breach* notifications required. **Organization** will request copies of any notifications to its *Individual*s, the public and *HHS* if **Organization**'s *individual*'s information was *breach*ed.
Record Keeping

Organization must keep records concerning all notifications, notices and postings made separately for each *Breach* reported. This includes any reports, notices or postings made by any other party on which **Organization** relied for its own notice to *individual*s, agencies, authorities, or media. These records must be kept for a minimum of six years following the provision of the notice, report or posting. If desired, utilize the *Breach* Notification Documentation Job Aid to record the details for recordkeeping.

RELEVANT *HIPAA* REGULATIONS:

- 45 CFR 164.404 *Notification to Individuals*
- 45 CFR 164.406 *Notification to the Media*
- 45 CFR 164.408 *Notification to the Secretary*
- 45 CFR 164.410 *Notification by a Business Associate*
- 45 CFR 164.412 *Law Enforcement Delay*
- 45 CFR 164.414 *Administrative Requirements and Burden of Proof*
- 45 CFR 164.530 *Administrative Requirements*

Glossary

Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to "*Access*" as used in this subpart, not as used in the HIPAA Breach Notification Rule or the HIPAA Privacy Rule).

Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of *security measures* to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.

Authentication means the corroboration that a person is the one claimed.

Availability means the property that data or information is *Access*ible and useable upon demand by an authorized person.

Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes.

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

ePHI means any protected health information (PHI) that is created, stored, transmitted, or received in any electronic format or media.

Facility means the physical premises and the interior and exterior of a building(s).

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner.

Malicious software means software, for example, a virus, designed to damage or disrupt a system.

Password means confidential *authentication* information composed of a string of characters.

Physical safeguards are physical measures, policies, and procedures to protect a covered entity's or business associate's electronic *information system*s and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Security or Security measures encompass all of the administrative, physical, and *technical safeguards* in an *information system*.

Security incident means the attempted or successful unauthorized *Access*, use, disclosure, modification, or destruction of information or interference with system operations in an *information system*.

Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control *Access* to it.

User means a person or entity with authorized *Access*.

Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

