HIPAA SECURITY POLICY & PROCEDURE MANUAL

Prepared By: Lisa Mootz
May 27th 2020

HIPAA SECURITY POLICY & PROCEDURE MANUAL

Jones County Iowa

Company Name: Will be referred as [Organization] throughout each policy.	**Jones County Iowa**
Policy Name:	Security Policy
Policy Version:	Version 1.0
Effective Date:	05/27/2020
Review Date:	Yearly
Security Officer: Will be referred as Security Officer throughout each policy.	Lisa Mootz
Privacy Officer: Will be referred as Privacy Officer throughout each policy.	Jenna Lovaas & Kaci Ginn
Compliance Officer: Will be referred as Compliance Officer throughout each policy.	Jenna Lovaas & Kaci Ginn
Responsible for Review:	Lisa Mootz/Jenna Lovaas & Kaci Ginn

TABLE OF CONTENTS

Security Manual Synopsis

This section is for all employees to review and attest. Below is a summary of each policy, including the relevant HIPAA regulations. 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 manual are included in the Glossary at the end of the manual.

Security 1.0 Assigned Security Responsibility

Organization shall have one individual identified and assigned to HIPAA security responsibility (the "HIPAA Security Officer").

The HIPAA Security Officer is responsible for ensuring the **organization's** HIPAA Security Rule policies and procedures are implemented and followed in each department.

§164.308(a)(2) *Assigned security responsibility*

Security 2.0 User Access Management

Organization must safeguard the confidentiality, integrity, and availability of electronic protected health information. To do this, the **organization** must manage who can access ePHI, implementing **user access** measures.

Before users are given access, the **organization** must train users in basic information security awareness. Once prerequisites have been satisfied, management and supervisors shall grant access to employees, under specific rules set forth in this policy. Access must be limited to what is necessary for a workforce member to perform his or her job.

Managers and supervisors must modify or terminate access when access has been compromised, is no longer needed, or when an employee terminates or is absent from employment. Under certain circumstances, management may grant itself emergency access, or may grant emergency access to individuals who have yet to complete training.

The **organization** must routinely review user access rights to ensure continuous compliance with this policy. Upon such review, the **organization** must update or modify user access rights, as necessary.

§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*

§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*
§164.312(a)(1) *Access control*
§164.312(c)(1) *Integrity*
§164.312(a)(2)(ii) *Emergency access procedure*

Security 3.0 Authentication & Password Management

Passwords are the first line of defense in protecting user accounts and the information contained in those accounts. All workforce members are required to comply with the Authentication & Password Management policy to ensure that their passwords are strong enough to protect the sensitive information in user accounts.

The policy consists of:

- Standards of Authentication – Verification
- The rules for maintaining Unique User ID and Password Management
- The guidelines for appropriate User ID and Passwords

Organization shall implement unique user IDs that are different from the **organization's** email address. Password guidelines, which incorporate best practices from the latest National Institute of Standards and Technology (NIST) guidelines (set forth in NIST SP 800-63B) are set forth below, and shall be used by **organization.**

1. Passwords shall be a minimum of eight (8) characters in length, and be a maximum length of at least 64 characters.
2. **Organization** and its workforce shall have the ability to use all special characters. **Organization** does not require that special characters be used. However, passwords shall be restricted as follows:
    a. Use of sequential and repetitive characters (i.e., 12345 or aaaaa) shall be restricted.
    b. Use of context-specific passwords (i.e., name of organization site) shall be restricted.
    c. Use of commonly used passwords (i.e., p@ssw0rd, etc.) shall be restricted.
    d. Passwords obtained from previous security breaches shall not be used.
3. Password protection requirements for users:
    a. Never reveal a password over the phone to anyone;
    b. Never reveal a password in an email message;
    c. Never reveal a password to your supervisor;
    d. Never talk about a password in front of others;
    e. Never hint at the format of a password (i.e., "my family name");
    f. Never reveal a password on questionnaires or security forms;

g. Never share a password with family members;
h. Never reveal a password to co-workers;
i. Never write down your password; instead, memorize it;
j. Never keep a list of user IDs and passwords in your office; and
k. Never misrepresent yourself by using another person's user ID and password.

§164.312(c)(2) *Mechanism to authenticate electronic protected health information*
§164.312(d) *Person or entity authentication*
§164.308(a)(5)(ii)(D) *Password management*
§164.312(a)(2)(i) *Unique user identification*

Security 4.0 Facility Access Controls

The **organization** must develop and implement facility access controls. These controls are a series of measures to reasonably safeguard ePHI stored in a physical location or its equipment.

Safeguard measures under a facility security plan include controlling workforce and visitor access; proper use and securing of metal/hard keys, network closets, server rooms, alarm systems, and doors. These measures are required to prevent unauthorized physical access and theft.

These procedures allow facility access to appropriate persons, so they can access data in an emergency.

When a facility undergoes repairs or modifications, these modifications must be logged and tracked, in accordance with this policy. When **organization** remodels existing sites or designs a new facility, it must revise its existing facility security plans, or create new ones, accordingly. All new and revised facility security plans must be evaluated on an ongoing basis and approved by **organization's** compliance officers.

The **organization** must conduct annual facility audits. These audits must ensure that ePHI safeguards for existing sites are being continuously maintained.

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

Security 5.0 Workstation Access Controls

The **organization must adequately shield** all observable ePHI from unauthorized disclosure or access on computer screens. **Organization's** workforce members must ensure that ePHI and other confidential information on computer screens is not visible to unauthorized persons.

Since ePHI is portable, workforce members must protect ePHI in *all* locations, including, but not limited to, homes or client sites.

The policy covers specific requirements for:

- Workforce members who work in other facilities.
- Workforce members who work from home or other non-office sites.
- Password protection of workforce member personal computers.
- Security for all other forms of portable ePHI, such as locking up CD ROM Disks, floppy disks, USB drives, PDAs, and laptops.
- Automatic, time-based user session-lock when a computer or workstation is left idle.
- Accessing (by, i.e., VPN) ePHI outside **organization's** Wide Area Network (WAN).

Workforce Member Requirements:

- Session lock the computer when it is left unattended;
- Ensure the computer is set to automatically lock when the computer is not in use;
- Ensure that no confidential information is viewable by unauthorized persons; and
- When working from home or other non-office work sites, protect ePHI from unauthorized access or viewing.

§164.310(a)(2)(iii) *Access control and validation procedures*
§164.310(b) *Workstation use*
§164.310(c) *Workstation security*
§164.312(a)(2)(iii) *Automatic log off*

Security 6.0 Device and Media Controls

ePHI stored or transported on storage devices and removable media, such as thumb drives and external hard drives, must be properly controlled and managed. Media containing PHI must also be properly backed up and disposed of.

Workforce Responsibilities:

1. Individual workforce members shall track laptops, PDAs, CD ROM Disks, and floppy disks, and all other portable media that contain ePHI.
2. To limit the amount of portable ePHI, workforce members shall not save any ePHI onto floppy disks, CD ROMs, and other portable items when it is not necessary.
3. Workforce members shall remove and destroy all ePHI before disposing of the media.

§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 7.0 Audit Controls

Organization's IT team must conduct a security audit on **organization's** computing resources.

Audits let the IT Team know whether safeguards are working. Audits may be conducted to:

1. Ensure integrity, confidentiality, and availability of information and resources.
2. Investigate possible security incidents to ensure conformance to **organization's** IT and security policies.
3. Monitor user or system activity where appropriate.
4. Verify that software patching is being maintained at the appropriate security level.
5. Verify that virus protection is being maintained at current levels.

§164.308(a)(5)(ii)(C) *Log-in monitoring*
§164.308(a)(1)(ii)(D) *Information system activity review*
§164.312(b) *Audit controls*

Security 8.0 Incident Response & Reporting

Organization must identify, track, respond to, and report security incidents. In addition, **organization** must mitigate the harmful effects of such incidents.

Workforce Members:
Workforce members are responsible for promptly reporting any security-related incidents to the Security Officer.

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

Security 9.0 Transmission Security

Organization must guard against unauthorized access to, or modification of, ePHI transmitted over an electronic communications network ("data in motion"). Organization shall commit resources to ensure that when ePHI is transmitted from one point to another, the ePHI is sufficiently protected to mitigate associated risk. Encryption measures play vital role in protecting ePHI.

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

Security 10.0 Protection from Malicious Software

The **organization** must install and maintain anti-virus software on computers it owns, leases, and/or operates; and configure all workstations to activate and update anti-virus software automatically, each time the computer is turned on, or, when a user logs onto the network. If a virus, worm, or other malicious code has infected or been identified on a server or workstation, organization must minimize the damage such code may cause. Workforce members must maintain cyber-hygiene standards.

Workforce Responsibilities:

1. Workforce members who utilize laptops to log on to the network shall work with their IT support to ensure all updates are received.
2. Workforce members shall not disable automatic virus or automatic malware scanning features.
3. All **non-organization** computers that directly access the WAN shall have anti-virus software and anti-malware software, and remain current with updates.
4. All downloaded files shall be malware-checked and virus-checked prior to use.
5. All storage media (i.e., disks) shall be treated as if they contain viruses or malware. Workforce members are permitted to use removable storage disks provided that all disks are virus-checked and malware-checked prior to use.
6. If a virus or malware is detected, workforce members are instructed to immediately contact their Security Officer.
7. For the purposes of protecting data and preventing the spread of malware, workers shall:
    - Attend HIPAA Security Training; and
    - Maintain back-up copies of data files.

§164.308(a)(5)(ii)(B) *Protection from malicious software*

Security 11.0 Contingency Plan, Disaster Recovery

Disasters and other emergencies may disrupt business continuity. Disasters include active hurricanes, tornadoes, shooter situations, war, and acts of terrorism. Other emergencies include fire, flood, pandemic, or outbreak. Organization must be prepared to respond to emergencies by creating, evaluating, testing and updating contingency plans. Contingency measures include:

- Applications and data criticality analysis;
- Data backup;
- Disaster Recovery Plan; and
- Emergency Mode Operation Plan.

§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 12.0 Business Associates

Business associates perform services for **organization** involving access to electronic protected health information. Such relationships must be formalized in a legally binding contract called a business associate agreement. Business associate performance under these agreements must be monitored. **Organization** must act on complaints it receives about business associates.

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

Security 13.0 Monitoring and Effectiveness

Organization must periodically evaluate its compliance with HIPAA security standards, by conducting security assessments. Assessments determine whether security controls have been properly implemented. When risk assessments are complete, **organization** will conduct risk management to remediate flaws revealed by the assessment.

§164.308(a)(8) *Perform a periodic technical and non-technical evaluation*
§164.308(a)(1)(i) *Security management process*
§164.308(a)(1)(ii)(A) *Risk analysis*
§164.308(a)(1)(ii)(B) *Risk management*

Security 14.0 Security Awareness and Training

All members of **organization's** workforce who can access ePHI must receive training needed to:

- Implement and maintain the **organization's** HIPAA Security Policies and Procedures; and
- Comply with the HIPAA Security Rule.

Security Awareness Training is key to eliminating the **organization's** exposure to both malicious threats and accidental errors and omissions.

§ 164.308(a)(5)(i) *Security awareness and training*
§ 164.308(a)(5)(ii)(A) *Security reminders*

Security 15.0 Sanctions Policy

Sanctions, penalties, and disciplinary actions must be applied against workforce members who fail to comply with security policies and procedures. Workforce members must report security incidents. Workforce members are protected from retaliation for reporting such incidents.

§ 164.308(a)(1)(ii)(C) *Sanction policy*

Security 16.0 Policies and Procedures

Organization must develop, and implement HIPAA Security Rule policies and procedures. These procedures must be revised when changes in regulations or changes in the work environment take place. These policies and procedures must be regularly reviewed. Reviews must be documented.

§ 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 17.0 Satellite Office and Home Office Policy

Satellite and Home Offices are offices that directly perform services for covered entities or business associates. PHI may not be stored in these offices. Devices used in these offices must be protected and encrypted.

Security 18.0 Work from Home Policy

Telecommuting is a voluntary work arrangement that allows employees to perform their jobs at home as part of the regular workweek. Employees who telecommute must observe proper security procedures.

Security 19.0 Bring Your Own Device Policy

Organization may allow employees to conduct work using their personally-owned devices to access **organization's** resources and services. Employees must take proper security precautions so the security and integrity of **organization's** data and technology infrastructure remains maintained.

Continued on Next Page

Security 1.0 Assigned Security Responsibility

FULL POLICY LANGUAGE:

Policy Purpose:

At all times, **organization** shall have one individual identified and assigned to HIPAA security responsibility (the "HIPAA Security Officer").

Policy Description:

The HIPAA Security Officer is responsible for **organization's** compliance with the HIPAA Security Rule. The HIPAA Security Officer is responsible for ensuring that **organization's** HIPAA Security Rule policies are implemented and followed.

Responsibilities include:

1. Ensuring that the necessary and appropriate HIPAA related policies are developed and implemented. These policies must provide for safeguarding the integrity, confidentiality, and availability of electronic protected health information (ePHI) within the **organization**.
2. Ensuring that the necessary infrastructure of personnel, procedures, and systems are in place:
    a. To develop and implement the necessary HIPAA policies;
    b. To monitor, audit, and review compliance with all HIPAA policies; and
    c. To provide a mechanism for reporting incidents and HIPAA security violations.
3. Acting as a spokesperson and single point of contact for the **organization** with respect to all HIPAA security issues**.**
4. Fulfilling all other duties documented within Security Officer's written job description and job title (which documentation shall be created by **organization)**.

Policy Responsibilities:

All HIPAA Security Officer responsibilities shall be assigned to this person.

The HIPAA Security Officer shall carry out the assigned responsibilities in coordination with their Job Description.

RELEVANT HIPAA REGULATIONS:

- § 164.308(a)(2) *Assigned security responsibility*

Security 2.0 User Access Management

FULL POLICY LANGUAGE:

Policy Purpose:

The intent of this policy is to establish rules for authorizing access to areas where ePHI is accessible. These areas include, but are not limited to, the computing network, applications, and workstations. Workforce members requiring access to ePHI will need authorization to work with ePHI in locations in which it resides.

This workforce security policy ensures that only workforce members who require access to ePHI for work-related activities shall be granted access. When work activities no longer require access, authorization shall be terminated. In addition, this policy provides guidelines on how workforce access is routinely reviewed and updated.

Policy Description:

Management and Access Control:
Only the workforce member's supervisor or manager can grant access to the **organization's** ePHI information systems.

Access to the information system or application may be revoked or suspended, consistent with the **organization's** policies and practices, if there is evidence that an individual is misusing information or resources.

Any individual whose access is revoked or suspended may be subject to disciplinary action or other appropriate corrective measures.

Minimum Necessary Access:
The **organization** shall ensure that only those workforce members who require access to ePHI are granted access. Each supervisor or manager is responsible for ensuring that the access to ePHI granted to each of his or her subordinates is the minimum necessary amount of access required for each subordinate's job role and responsibilities. If the subordinate no longer requires access, it is the supervisor or manager's responsibility to complete the necessary process to terminate access.

Granting Access to ePHI:

- **Screen Workforce Members Prior to Access:**
  The manager or supervisor shall ensure that information access is granted only after verifying that the access of a workforce member to ePHI is necessary and appropriate.

- **Sign Security Acknowledgement:**

Prior to being issued a User ID or logon account to access any ePHI, each workforce member shall sign the **organization's** Confidentiality Agreement, and shall thereafter comply with all of **organization's** security policies and procedures.

- **Security Awareness Prior to Getting Access:**
  Before access is granted to any of the various systems or applications that contain ePHI, workforce members shall be trained to a minimum standard. Topics to be covered in training will 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.

- **Management Approval:**
  The **organization** shall implement the following policies:

  1. User IDs or logon accounts may only be assigned with management approval.
  2. Managers are responsible for requesting the appropriate level of computer access for staff to perform their job functions.
  3. All requests regarding User IDs or computer system access for workforce members must be to be communicated to the appropriate individuals by email. This allows requests to be tracked.
  4. System administrators must process only those requests that have been authorized in writing by managers.
  5. The system administrator must retain requests for a minimum of one (1) year.

Granting Access in an Emergency:

- **Emergency User Access:**
  Management has the authority and discretion to grant emergency access for workforce members who have not completed the steps listed in the "Granting Access to ePHI" section above if:

  1. The **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.
  2. Management determines that granting immediate access is in the best interest of the client whose ePHI may be exposed. The reason(s) for this determination should be documented.

If management grants emergency access, the granting of access shall be documented and reviewed within 24 hours.

After the emergency event is over, the user access shall be removed. The workforce member shall then complete the normal requirements for being granted access.

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

  1. The workforce member is terminated or resigns, and management requires access to the person's data;
  2. The workforce member is on approved leave of absence for a prolonged period;
  3. The workforce member has not been in attendance and therefore is assumed to have resigned; or
  4. The workforce member's superior needs immediate access to data on a workforce member's computer to provide client treatment.

Termination of Access:
Department managers or their designated representatives are responsible for terminating 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 systems or resources in a manner inconsistent with **organization's** HIPAA Security Rule policies.
2. If the workforce member or management has evidence or reason to believe the user's password has been compromised.
3. If the user resigns, is terminated, is suspended, retires, or is away on unapproved leave.
4. If the user's job description changes and system access is no longer justified by the new job description.

If a workforce member's employment is terminated, the workforce member's access to ePHI shall be terminated in accordance with the terms of the "Policy Responsibilities" section, below.

If the workforce member is on an approved leave of absence for more than three weeks, management shall suspend the user's account until the workforce member returns from his or her leave of absence.

Modifications to Workforce Member's Access:
If a workforce member transfers to another program or changes role(s) within the same program within the **organization:**

1. The workforce member's new supervisor or manager is responsible for promptly evaluating the workforce member's current access.
2. The workforce member's new supervisor or manager is responsible for requesting access to ePHI commensurate with the workforce member's new role and responsibilities.

Ongoing Compliance for Access:
To ensure that workforce members have access to ePHI only when it is required for their job function, the following measures shall be implemented by **organization:**

1. Every new User ID or log on account that has not been used for thirty (30) consecutive calendar days since creation shall be investigated to determine if the workforce member still requires access to the ePHI.
2. At least every six (6) months, IT teams are required to send to supervisors/managers (or appropriate designees):
    a. A list of all workforce members with access to all applications;
    b. A list of workforce members and their access rights for all shared folders that contain ePHI; and
    c. A list of all Virtual Private Network (VPN) workforce members.
3. The supervisors/managers shall then notify their IT teams of any workforce members that no longer require access or who require modified access.

Policy Responsibilities:

Security Officer or Designee Responsibilities:

1. The Security Officer shall, via email, provide the System Administrator with the names of workforce members who are terminating or transferring out of the **organization,** along with the applicable supervisor's name and the effective date of termination or transfer.
2. The Security Officer shall work with HR or its designee to arrange a process to immediately email and telephone IT and Facilities Management if a workforce member is being released from probation or has been terminated with cause. The HR division shall provide the workforce member's name, supervisor's name, and effective date, so that access can be discontinued when the personnel action is effective.

Organization's IT Team(s) Responsibilities - Account Management:

1. Upon written notification of access modification or termination, a user's access to ePHI shall immediately be modified or removed.

2. A monthly report shall be created that identifies new User IDs or log on accounts not accessed within thirty (30) days of creation. Managers shall be notified to determine whether these accounts should be removed.
3. The IT Team shall provide a report every six (6) months to the manager/supervisor or designee, documenting users with access to ePHI, and requesting verification that access is still required to fulfill the user's job functions.

Managers' and Supervisors' Responsibilities:

1. Each manager/supervisor is responsible for ensuring that the access to ePHI granted to each of their subordinates is the minimum necessary access required for each such subordinate's job role and responsibilities.
2. If the user no longer requires access, it is the manager/supervisor's responsibility to undertake the necessary measures as soon as possible to terminate access.
3. The manager/supervisor shall validate new User IDs or log on accounts that are not accessed within 30 days of creation. If access is no longer required, the User ID shall be deleted.
4. Managers/supervisors shall review and verify semi-annual user and folder access reports and VPN access reports prepared by the IT team, to determine if the workforce members still require access to ePHI.
5. The manager/supervisor shall ensure members of the workforce have signed the IT security agreement and are properly trained before approving access to ePHI.

User Responsibility:

Each user shall read and agree to comply with the **organization's** IT Security Policies, sign the **organization's** HIPAA Confidentiality Agreement, attend HIPAA Security training, and report all security incidents.

Procedures:

Organization shall document written procedures for granting user access, the authorization of access to ePHI, and the termination of user access. These procedures shall include, as a minimum, all of the policy requirements above.

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*
- §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*
- §164.312(a)(1) *Access control*
- §164.312(c)(1) *Integrity*

- §164.312(a)(2)(ii) *Emergency access procedure*

Continued on Next Page

Security 3.0 Authentication & Password Management

FULL POLICY LANGUAGE:

Policy Purpose:

Passwords are an important aspect of computer security and are the front line of protection of user accounts and the ePHI contained therein. A compromised password may result in a security breach of **organization's** network. All **organization** workforce members are responsible for taking the appropriate steps to select and secure their passwords. The purpose of this policy is to reinforce the use of effective passwords, also known as "strong passwords," and require workforce members to change their passwords on a regular basis.

Policy Description:

Information systems used to access ePHI shall uniquely identify and authenticate workforce members through the use of strong passwords.

Authentication – Verification:

Industry standard protocols will be used on all routers and switches used in the Wide Area Network (WAN) and the Local Area Networks (LANs). Authentication types can include:

1. Unique user ID and passwords;
2. Biometric identification system;
3. Telephone callback;
4. A token system that uses a physical device for user identification;
5. Two forms of authentication for wireless remote access; or
6. Information systems used to access ePHI shall use technology such as digital certificates, to identify and authenticate connections to specific devices involved in system communications.

The password file on the authenticating server shall be adequately protected and encrypted.

Unique User ID and Password Management:

1. All **organization** workforce members shall be assigned a unique user ID to access the network. All workforce members are responsible for creating and maintaining the confidentiality of the password associated with their unique user ID. Managers/supervisors are required to ensure that their staff understands the user responsibilities for securely managing confidential passwords.
2. Upon receipt of a user ID, the person assigned to this ID is required to change the password provided by the administrator to a password that only he or she (the user) knows. Effective passwords shall be created in order to secure access to electronic protected health information (ePHI).

3. Workforce members who suspect that their password has become known by another person shall change their password immediately. No user shall give his or her password to another person.
4. Workforce members are required to change all passwords every six months. Passwords that must be changed include: Network user ID passwords, and all application access passwords. Where technology is capable, network and application systems shall be configured to enforce automatic expiration of passwords every six months.
5. All privileged system-level passwords (i.e., root, enable, NT admin, application administration accounts, etc.) shall be changed at least each fiscal quarter. All passwords are to be treated as sensitive, confidential **organization** information.

User ID & Password Guidelines:
Organization shall implement unique user IDs that are different from the **organization's** email address. Password guidelines, which incorporate best practices from the latest National Institute of Standards and Technology (NIST) guidelines (set forth in NIST SP 800-63B) are set forth below, and shall be used by **organization.**

1. Passwords shall be a minimum of eight (8) characters in length, and be a maximum length of at least 64 characters.
2. **Organization** and its workforce shall have the ability to use all special characters. **Organization** does not require that special characters be used. However, passwords shall be restricted as follows:
    a. Use of sequential and repetitive characters (i.e., 12345 or aaaaa) shall be restricted.
    b. Use of context-specific passwords (i.e., name of organization site) shall be restricted.
    c. Use of commonly used passwords (i.e., p@ssw0rd, etc.) shall be restricted.
    d. Passwords obtained from previous security breaches shall not be used.

Organization shall implement the following additional password requirements:

1. Password selection software should not allow "obvious" passwords:
    a. Common words, words related to the user, repeated letters, numeric sequences, etc. (i.e., "password123", "johnsmith", or "abcabcabc").
2. Login software should include features to prevent brute force attacks, such as:
    a. Delays between login attempts; and
    b. Lock account after a reasonable number of failed attempts.
3. Password protection requirements for users:
    a. Never reveal a password over the phone to anyone;
    b. Never reveal a password in an email message;
    c. Never reveal a password to your supervisor;
    d. Never talk about a password in front of others;

e. Never hint at the format of a password (i.e., "my family name");
f. Never reveal a password on questionnaires or security forms;
g. Never share a password with family members;
h. Never reveal a password to co-workers;
i. Never write down your password; instead, memorize it;
j. Never keep a list of user IDs and passwords in your office; and
k. Never misrepresent yourself by using another person's user ID and password.

Policy Responsibilities:

Managers' and Supervisors' Responsibility:
Managers/supervisors are responsible to reinforce secure password use in their offices with emphasis on 'no password sharing'. If access to another worker's account is required, managers/supervisors shall follow the emergency access section of **organization's** HIPAA User Access Management policy.

IT Team(s) Responsibilities for Network User ID Creation:

1. System administrators shall provide the password for a new unique user ID to only the user to whom the new ID is assigned.
2. Workforce members may at times request that their password be reset. System administrators shall verify the identity of the user requesting a password reset or verify that the person making the request is authorized to request a password reset for another user. When technically possible, a new or reset password shall be set to expire on its attempted use at log on so that the user is required to change the provided password to one only they know.

All Workforce Members Accessing ePHI:
Any workforce member who suspects that their password has become known by another person shall change their password immediately.

Procedures:

Managers' and Supervisors' Responsibility:
Managers/supervisors are responsible to reinforce secure password use in their offices with emphasis on 'no password sharing'. If access to another worker's account is required, managers/supervisors shall follow the emergency access section of **organization's** HIPAA User Access Management policy.

IT Team(s) Responsibilities for Network User ID Creation:

1. System administrators shall provide the password for a new unique user ID to only the user whom the new ID is assigned.
2. Users may at times request that their password be reset. System administrators shall verify the identity of the user requesting a password reset or verify that the person making the request is authorized to request a password reset for another

user. When technically possible, a new or reset password shall be set to expire on its initial use at log on so that the user is required to change the provided password to one only they know.

All Workforce Members Accessing ePHI:
Any workforce member who suspects that their password has become known by another person shall change their password immediately.

RELEVANT HIPAA REGULATIONS:

- §164.312(c)(2) *Mechanism to authenticate electronic protected health information*
- §164.312(d) *Person or entity authentication*
- §164.308(a)(5)(ii)(D) *Password management*
- §164.312(a)(2)(i) *Unique user identification*

Continued on Next Page

Security 4.0 Facility Access Controls

FULL POLICY LANGUAGE:

Policy Purpose:

To describe the physical safeguards **organization** shall implement to safeguard ePHI from any intentional or unintentional use or disclosure.

Policy Description:

General:

Organization shall reasonably safeguard ePHI from any intentional or unintentional use or disclosure. Organization shall implement physical safeguards to protect its facilities where ePHI can be accessed. Such safeguards shall maintain the confidentiality, integrity, and availability of ePHI.

New or Remodeled Facility for Organization:

When designing a new building and remodeling existing sites, facility managers and/or designees shall work with the Security Officer(s) to ensure the facility plan components below are compliant with the HIPAA Regulations.

Facility Security Plan:

Organization shall safeguard its facilities and the equipment therein from unauthorized physical access, tampering, and theft. **Organization's** Security Officer(s) shall annually audit **organization's** facilities to ensure ePHI safeguards are continuously being maintained.

Facility Security Guidelines for the Workforce:

1. Do not share access cards to enter the facility;
2. 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);*
3. Do not share hard key access to enter the facility; and
4. Do not share alarm codes or keypad codes to enter the facility.

One or more of the following shall be implemented for all sites that access ePHI:

1. **Visitor Access Control:** In facilities where ePHI is available, all visitors shall be escorted and monitored. Each facility shall implement its own procedures that govern visitor access controls. These procedures may vary depending on the facilities structure, the type of visitors, and where the ePHI is accessible.
2. **Metal/Hard Keys:** Facilities that use metal/hard keys shall change affected or appropriate key locks when keys are lost or a workforce member leaves without returning the key. In addition, the facility shall have:

a. Clearances based on programmatic need, special mandated security requirements and workforce member security; and
b. A mechanism to track which workforce members are provided access.

3. **Network Closet(s):** Every network closet shall be locked whenever the room is unoccupied or not in use. **Organization** shall document who has access to the network closets and periodically change the locking mechanisms.
4. **Server Room(s):** Every server room shall be locked whenever the room is unoccupied or not in use. The **organization** shall document who has access to each server room and periodically change the locking mechanisms.
5. **Alarm Systems:** All buildings that have ePHI shall have some form of alarm system that is activated during non-business hours. Alarm system codes may only be provided to workforce members that require this information in order to leave and enter a building. These alarm codes shall be changed at least every six (6) months.
6. **Doors**: All external facility doors and doors to areas where ePHI is housed shall remain completely shut at all times. It is each workforce member's responsibility to make sure the door that is being entered or exited is completely shut before leaving the vicinity. Sometimes the doors do not completely close by themselves. If a door's closing or locking mechanism is not working, it is every worker's responsibility to notify the facility manager or designee for that facility.

Contingency Operations - Emergency Access to Facilities:
Each facility shall have emergency access procedures in place that allow facility access to appropriate persons to access data. This includes a primary contact person and back-up person for when facility access is necessary after business hours by persons who do not currently have access to the facility.

Maintenance Records Policy:
Repairs or modifications to the physical building for each facility where ePHI can be accessed shall be logged and tracked. These repairs are tracked centrally by Facility Management (i.e., building manager, landlord, maintenance). The log shall include events that are related to security (for example, repairs or modifications of hardware, walls, doors, and locks).

Policy Responsibilities:

Manager/Supervisor Requirements:

1. Take appropriate corrective action against any person who knowingly violates the facility plan;
2. Authorize clearances that are appropriate to the duties of each workforce member;
3. Notify the security administrator or designee within one (1) business day when a user no longer requires access to the facility; and
4. Verify that each worker surrenders her/his card or key upon ending employment with **organization.**

Worker Requirements:

1. Display their access/security card to demonstrate their authorization to access restricted areas;
2. Immediately report lost or stolen (key/ID) cards, or metal keys or keypad-cipher lock combinations; and
3. Surrender access card or key upon leaving employment.

Facility Manager/Security Officer or Designee Requirements:

1. Request and track maintenance repairs;
2. Establish and maintain a mechanism for accessing the facility in an emergency;
3. Track who has access to the facility;
4. Change metal locks when a key is lost or unaccounted for;
5. Change combination keypads/cipher locks every three (3) months;
6. Change the alarm code every six (6) months;
7. Disable access cards not used for 90 days or more; and
8. Complete access card audits every six (6) months to verify user access.

Security Officer Responsibilities:

1. Work with Facility Management and **organization** to ensure facilities comply with the HIPAA Security Rule for facility access controls; and
2. Conduct annual audits of **organization's** facilities to ensure the facility is secured and the requirements of this policy are being enforced.

Procedures:

Organization shall document written procedures for their facility security plan. Procedures shall be written to address the unique requirements of each facility. An essential part of compliance is to document and implement processes to ensure the safeguards in the facility security plan are being maintained.

Organization shall submit new and revised procedures and plans to the Security Officer(s) for approval and ongoing evaluation. Any procedures developed by **organization** shall be consistent with **organization's** HIPAA policies and not deviate from **organization's** standards.

RELEVANT HIPAA REGULATIONS:

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

Security 5.0 Workstation Access Controls

FULL POLICY LANGUAGE:

Policy Purpose:

This policy outlines processes **organization** and its workforce must use to shield ePHI from unauthorized, incidental, or accidental workstation viewing.

Policy Description:

Workstation Use:

1. Workforce members shall ensure that observable ePHI is adequately shielded from unauthorized disclosure and unauthorized access on computer screens. **Organization** and its workforce shall make every effort to ensure that ePHI and any other confidential information on computer screens is not visible to unauthorized persons.
2. Workforce members working in facilities that are not part of **organization** shall maintain awareness of their surroundings to ensure that no one can incidentally view ePHI, and that no ePHI is left unattended.
3. Workforce members who work from home or other non-office sites shall take the necessary steps to protect ePHI from other persons who may have access to their home or other non-office site. These measures include password protection of their personal computers, and security measures for all other forms of portable ePHI such as locking up CD ROM Disks, floppy disks, USB drives, PDAs, and laptops.
4. User session-lock shall be implemented when the computer is left idle. It shall be automatic after a specified time based on location and function. The session shall be locked to disable access to the PC until the user enters their unique password with login information.
5. While accessing ePHI outside the **organization's** Wide Area Network (for example: extranet, VPN), automatic log off shall occur after a maximum of 15 minutes of inactivity. Automatic log off is a system-enabled enforcement of session termination after a period of inactivity and blocks further access until the workforce member reestablishes the connection using the identification and authentication process.

Policy Responsibilities:

Manager/Supervisor Requirements:

1. Take appropriate corrective action against any person who knowingly violates the security requirements associated with workstation use;
2. Ensure that workers set their computers to automatically lock when the computer is not in use; and
3. Ensure that no confidential information is viewable by unauthorized persons at workstations in offices under their management.

Workforce Member Requirements:

1. Session lock the computer when it is left unattended;
2. Ensure the computer is set to automatically lock when the computer is not in use;
3. Ensure that no confidential information is viewable by unauthorized persons; and
4. When working from home or other non-office work sites, protect ePHI from unauthorized access or viewing.

IT Support:

1. When installing new workstations, set the session lock timer to lock the computer when left unattended; and
2. When installing new systems or applications, set the automatic log off timer to terminate the session when the computer is left unattended.

Procedures:

Procedures for protecting workstations include:

1. Use of polarized screens or other computer security screen overlay devices that shield confidential information;
2. Placement of computers out of the visual range of persons other than the authorized user;
3. Clearing confidential information from the screen when it is not actively in use;
4. Setting an automatic session lock option on all computer workstations;
5. Shutting down or locking workstation sessions when left unattended; and
6. When the technology is capable, setting the applications to automatically log off after a specific time of inactivity.

Organization shall develop and implement procedures to ensure confidentiality of ePHI. **Organization** shall submit all new and revised procedures to the Security Officer for approval and ongoing evaluation. Any procedures developed by **organization** shall be consistent with **organization's** HIPAA policies and not deviate from **organization's** standards.

RELEVANT HIPAA REGULATIONS:

- §164.310(a)(2)(iii) *Access control and validation procedures*
- §164.310(b) *Workstation use*
- §164.310(c) *Workstation security*
- §164.312(a)(2)(iii) *Automatic log off*

Security 6.0 Device and Media Controls

FULL POLICY LANGUAGE:

Policy Purpose:

The intent of this policy is to ensure that ePHI stored or transported on storage devices and removable media is appropriately controlled and managed.

Policy Description:

Device and Media Controls/Accountability:

1. **Organization** shall protect all hardware and electronic media that contains electronic protected health information (ePHI). This includes personal computers, PDAs, laptops, storage systems, backup tapes, CD ROM disks, and removable disks.
2. Every area of the **organization** is responsible for developing procedures that govern the receipt and removal of hardware and electronic media that contain(s) ePHI into and out of a facility. Procedures shall include maintaining a record of movements of electronic media with ePHI and any persons responsible for its transportation.

Portable Media Use – Security:

1. In addition to protecting **organization's** workstations and facilities, workforce members shall protect ePHI when working from all other locations. This includes, but is not limited to, home, other offices, or when working in the field.
2. In order to limit the amount of portable ePHI, workforce members shall not save any ePHI on floppy disks, CD ROM disks, or other portable items.
3. Methods for protecting portable media with ePHI include:
    a. All workforce members shall receive permission from their supervisor before removing ePHI from their facility. Approvals shall specify the type of permission and the time period for authorization, not to exceed one (1) year.
    b. Workforce members who work in the field shall not leave ePHI unlocked or visible in their vehicles. In addition, these workforce members may not leave any ePHI in client facilities/homes.
    c. If ePHI is lost, workforce members are responsible for promptly contacting their supervisor, the Security Officer, or designated Compliance Officers responsible for HIPAA Compliance within one (1) business day of awareness that ePHI has been lost.

Disposal:

Before electronic media that contains ePHI can be disposed, the following actions shall be taken on all computers containing ePHI:

1. Hard drives shall be either wiped clean or destroyed. Hard drive cleaning, if chosen, shall meet the Department of Defense (DOD) standards, which require, *"The method*

of destruction shall preclude recognition or reconstruction of the classified information or material." Another method for removal of ePHI from hard drives is known as purging. Purging includes degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains.

a. In addition, the hard drive, once cleaned, shall be tested to ensure the information cannot be retrieved.
b. Backups shall also be destroyed or returned to the owner and their return documented. Destruction must ensure there is no ability to reconstruct the data.
c. Other media, such as memory sticks, USB flash drives or micro drives, CD-ROMs and floppy disks, shall be physically destroyed (i.e., broken into pieces, pulverized, or shredded by a shredder that can perform this function) before disposing of the item.

Media Reuse:

1. All ePHI shall be removed from hard drives when the equipment is transferred to 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. Hard drives shall be wiped clean before transfer.
2. Cleaning shall meet the Department of Defense (DOD) standards as outlined above. In addition, the hard drive, once cleaned, shall be tested to ensure the information cannot be retrieved.

Sending a Computer Server Hard Drive to Repair:
As technology permits, before **organization** sends a device out for repair, an exact copy of ePHI shall be created, and ePHI shall be removed from the server hard drive.

Moving Computer Server Equipment with ePHI:
Before moving server equipment that contains ePHI, a retrievable exact copy shall be created.

Device and Media Acquisition:
The **organization**, when acquiring information systems, shall ensure those systems meet the **organization's** security requirements and/or security specifications. Information Systems (applications, servers, copiers, etc.) acquisition requires an assessment of risk.

Policy Responsibilities:

Manager/Supervisor Responsibilities:
Ensure that only workforce members who need to remove ePHI from their facilities are granted permission to do so. Such permission, when given, must be within the parameters of this policy.

IT Responsibilities:

1. Ensure all hard drives are wiped clean before disposal or reuse.
2. Test hard drives to ensure they are clean.
3. Before moving hardware or sending hard drives for repair that contain ePHI, create a retrievable copy of ePHI data and wipe the hardware or hard drive.
4. Maintain an inventory and a record of movements or transfers of hardware and electronic media such as workstations, servers, or backup tapes.

Workforce Responsibilities:

1. Individual workforce members shall track laptops, PDAs, CD ROM Disks, and floppy disks, and all other portable media that contain ePHI.
2. To limit the amount of portable ePHI, workforce members shall not save any ePHI onto floppy disks, CD ROMs and other portable items when it is not necessary.
3. Workforce members shall remove and destroy all ePHI before disposing of the media.

Procedures:

The **organization** shall document written procedures to track, dispose, and reuse media devices used for ePHI. The **organization** shall submit all new and revised procedures to the Security Officer for approval and ongoing evaluation. Any procedures developed by the **organization** shall be consistent with the **organization's** HIPAA policies and not deviate from the organization's standard.

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*

Continued on Next Page

Security 7.0 Audit Controls

FULL POLICY LANGUAGE:

Policy Purpose:

The purpose of this policy is to outline mechanisms that ensure servers, workstations, and other computer systems are appropriately secured through proper audit controls.

Policy Description:

Log-in Monitoring:

1. The **organization** has the right to monitor system access and activity of all workforce members.
2. To ensure that access to servers, workstations, and other computer systems containing ePHI is appropriately secured, the following login monitoring measures shall be implemented:
    a. A mechanism to log and document four (4) or more failed log-in attempts in a row shall be implemented on each network system containing ePHI when the technology is capable.
    b. Login activity reports and logs shall be reviewed, at a minimum, on a biweekly basis, to identify any patterns of suspicious activity.
    c. All failed login attempts of a suspicious nature, such as continuous attempts, shall be reported immediately to the Security Officer or the designee for the **organization**.
    d. To the extent that technology allows, any user ID that has more than four (4) repeated failed login attempts in a row shall be disabled for a minimum of 30 minutes.

Information System Activity Review – Audit Controls:

To ensure that activity for all computer systems accessing ePHI is appropriately monitored and reviewed, these requirements shall be met:

1. Where technology allows, the audit record shall capture sufficient information to establish what events occurred, the sources, and the outcomes of the events.
2. Every application and system administrator or designee shall be reviewed, at a minimum, once each fiscal quarter, audit logs, activity reports, or other mechanisms to document and manage system activity.
3. Indications of improper use shall be reported to management for investigation and follow up.
4. Audit logs of access to networks and applications with ePHI shall be archived.
5. Audit information and audit tools shall be protected from unauthorized access, modification, and deletion.

Policy Responsibilities:

System administrators and Security Officers are responsible to implement and monitor audit controls for all systems that contain ePHI.

Procedures:

The **organization** shall submit all new and revised procedures to the Chief Compliance Officer for approval and ongoing evaluation. The Security Officer shall create audit control checklists and logs to assist with, and standardize, the audit function. Any procedures developed by the **organization** shall be consistent with its HIPAA policies and not deviate from the **organization's** standards.

RELEVANT HIPAA REGULATIONS:

- §164.308(a)(5)(ii)(C) *Log-in monitoring*
- §164.308(a)(1)(ii)(D) *Information system activity review*
- §164.312(b) *Audit controls*

Continued on Next Page

Security 8.0 Incident Response & Reporting

FULL POLICY LANGUAGE:

Policy Purpose:

The purpose of this policy is to formalize the response to, and reporting of, security incidents. This includes identification and response to suspected or known security incidents, the mitigation of the harmful effects, and the documentation of security incidents and their outcomes.

Policy Description:

Organization shall employ tools and techniques (including, but not limited to, The Guard and its Process) to monitor events, detect attacks, and provide identification of unauthorized use of the systems that contain ePHI.

Reporting:

1. All security incidents, threats, or violations that affect or may affect the confidentiality, integrity, or availability of ePHI shall be reported and responded to promptly.
2. Incidents to be reported include, but are not limited to:
    a. Virus, worm, ransomware, or other malicious code attacks;
    b. Network or system intrusions;
    c. Persistent intrusion attempts from a particular entity;
    d. Unauthorized access to ePHI, an ePHI based system, or an ePHI based network;
    e. ePHI data loss due to disaster, failure, error, or theft;
    f. Loss of any electronic media that contains ePHI;
    g. Loss of the integrity of ePHI; and
    h. Unauthorized person(s) found in the **organization's** facility.
3. The **organization's** Compliance Officer shall be notified immediately of any suspected or real security incident. If it is unclear as to whether a situation is a security incident, the Compliance Officer shall be contacted to evaluate the situation.

Response and Resolution:

The Chief or Lead Compliance Officer (CCO/LCO), who supervises the Privacy Officer and the Security Officer, is the only person in **organization's** workforce that can resolve a security incident (In small organizations, the duties of the Privacy Officer, Security Officer, and CCO/LCO, are commonly performed by the same person).

The CCO/LCO shall track the incident and review reports provided by the Security Officer to determine if an investigation of the incident is necessary. The Compliance Officers shall also determine if a report of the incident should be forwarded to the Department of Health and Human Services (HHS). The CCO/LCO shall decide if the **organization's** Legal Counsel, Law Enforcement, Human Resources, or Communication and Media Office should be

informed and involved in the resolution of the incident. All HIPAA security-related incidents and their outcomes shall be logged and documented by the CCO/LCO Compliance Officers. The **organization** and its CCO/LCO will record all the incidents and retain these incident reports for six years.

Policy Responsibilities:

Violations of this policy shall be reported to the **organization**'s Chief Compliance Officer.

The Organization:
The **organization** shall train personnel in their incident response roles and responsibilities and provide refresher training as needed. The **organization** shall test the incident response capability at least annually using tests and exercises to determine the effectiveness.

Workforce Members:
Workforce members are responsible for promptly reporting any security-related incidents to the Security Officer.

IT Help Desk:
The Security Officer shall document all security incidents and provide reports to the CCO/LCO.

Compliance Officers:
The Chief Compliance Officer(s) that is responsible to determine if the incident requires further investigation**.** The **organization's** Security Officer and Privacy Officer shall determine if corrective actions should be implemented. The CCO/LCO is responsible for documenting the investigations and any corrective actions. The CCO/LCO is responsible for maintaining all documentation on security breaches for six (6) years.

Procedures:

The **organization** shall submit all new and revised procedures to the CCO/LCO for approval and ongoing evaluation. Any procedures developed by the **organization** shall be consistent with the **organization's** HIPAA policies and not deviate from the **organization's** standard HIPAA operating procedures.

RELEVANT HIPAA REGULATIONS:

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

Security 9.0 Transmission Security

FULL POLICY LANGUAGE:

Policy Purpose:

The intent of this policy is to guard against unauthorized access to, or modification of, ePHI that is being transmitted over an electronic communications network. When ePHI is transmitted from one point to another, it shall be protected in an encrypted manner. This policy also requires encryption of data at rest for all devices that connect to or store ePHI.

Policy Description:

Encryption:

Proven, standard algorithms shall be used as the basis for encryption technologies. The use of proprietary encryption algorithms is not allowed for any purpose unless authorized by the **organization's** HIPAA Security Officer.

Circumstances Where Encryption is Required:

1. All devices that connect to or store ePHI must be encrypted.
2. No ePHI shall be sent outside the **organization's** domain unless it is encrypted. This includes all email and email attachments sent over a public internet connection.
3. When accessing a secure network, an encryption communication method, such as a VPN, shall be used.

Circumstances Where Encryption if Optional:

1. When using point-to-point communication protocols to transmit ePHI, no encryption is required.
2. Dial-up connections directly into secure networks are considered to be secure connections for ePHI and no encryption is required.

Rules for Modem Use:

1. Modems shall never be left connected to personal computers in auto-answer mode.
2. Dialing directly into or out of a desktop computer that is simultaneously connected to a Local Area Network (LAN) or another internal communication network is prohibited.
3. Dial-up access to WAN-connected personal computers at the office is prohibited.

ePHI Transmissions Using Wireless LANs and Devices within the Organization Domain:

1. The transmission of ePHI over a wireless network within the **organization's** domain is permitted if both of the following conditions are met:
    a. The local wireless network is utilizing an authentication mechanism to ensure that wireless devices connecting to the wireless network are authorized; and

b. The local wireless network is utilizing an encryption mechanism for all transmissions over that wireless network and uses two (2) types of authentication.

2. If transmitting ePHI over a wireless network that is not utilizing an authentication and encryption mechanism, the ePHI shall be encrypted before transmission.

Perimeter Security:

1. Any external connection to the **organization's** Wide Area Network (WAN) shall come through the perimeter security's firewall.
2. If determined to be safe by the Security Officer, outbound services shall be initiated for internal addresses to external addresses.
3. Inbound services shall be negotiated on a case-by-case basis with the Security Officer.
4. All workforce members connecting to the WAN shall sign a Confidentiality Agreement before connectivity is established.

Firewall Controls to Transmit ePHI into and Out of Organization:

1. Networks containing systems and applications with ePHI shall implement perimeter security and access control with a firewall.
2. Firewalls shall be configured to support the following minimum requirements:
   a. Limit network access to only authorized workforce members and entities;
   b. Limit network access to only legitimate or established connections (an established connection is return - traffic in response to an application request submitted from within the secure network); and
   c. Console and other management ports shall be appropriately secured or disabled.
3. The configuration of firewalls used to protect networks containing ePHI based systems and applications shall be submitted to the Security Officer for review and approval.

Policy Responsibilities:

All workforce members that transmit ePHI when using the public internet or a wireless device outside the **organization** WAN, are responsible for ensuring the information is safeguarded by using encryption.

Procedures:

Each area of the **organization** shall submit all new and revised procedures to the Chief Compliance Officer/Lead Compliance Officer for approval and ongoing evaluation. Any procedures developed by the **organization** shall be consistent with the **organization's** HIPAA policies and not deviate from the **organization**'s privacy and security standards.

RELEVANT HIPAA REGULATIONS:

- §164.312(e)(1) *Transmission security*

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

Continued on Next Page

Security 10.0 Protection from Malicious Software

FULL POLICY LANGUAGE:

Policy Purpose:

The intent of this policy is to establish procedures for protections to guard against, detect, and report malicious software. Malicious software includes, but is not limited to viruses, worms, trojans, and ransomware attacks.

Policy Description:

The **organization** shall ensure all computers it owns, leases, and/or operates, are installed with, and maintain, anti-virus and anti-malware software. All workstations shall be configured to activate and update anti-virus and anti-malware software automatically each time the computer is turned on or the user logs onto the network.

In the event that a virus, worm, or other malicious code has infected or been identified on a server or workstation, that equipment shall be disconnected from the network until it has been appropriately disinfected.

Policy Responsibilities:

Workforce Responsibilities:

1. Workforce members who utilize laptops to log on to the network shall work with their IT support to ensure all updates are received.
2. Workforce members shall not disable automatic virus or automatic malware scanning features.
3. All **non-organization** computers that directly access the WAN shall have anti-virus software and anti-malware software, and remain current with updates.
4. All downloaded files shall be malware-checked and virus-checked prior to use.
5. All storage media (i.e., disks) shall be treated as if they contain viruses or malware. Workforce members are permitted to use removable storage disks provided that all disks are virus-checked and malware-checked prior to use.
6. If a virus or malware is detected, workforce members are instructed to immediately contact their Security Officer.
7. For the purposes of protecting data and preventing the spread of malware, workers shall:
    - Attend HIPAA Security Training; and
    - Maintain back-up copies of data files.

IT Responsibility:

Set up laptop computers so they automatically load malware updates when they are connected to the **organization's** network.

Procedures:

To ensure that all **organization** workforce members are made aware of the threats and vulnerabilities due to malicious code and software such as viruses and worms, and are effectively trained to identify and prevent these types of attacks, the following procedures shall be established and implemented:

1. The workforce shall be trained to identify and protect data, when possible, against malicious code and software.
2. Security reminders shall be given to the workforce to inform them of any new virus, worm, or other type of malicious code that may threaten ePHI.

The **organization** shall submit all new and revised procedures to the Chief Compliance Officer/Lead Compliance Officer for approval and ongoing evaluation. Any procedures developed by the **organization** shall be consistent with its HIPAA policies and not deviate from the **organization's** privacy and security standards set forth in those policies.

RELEVANT HIPAA REGULATIONS:

- §164.308(a)(5)(ii)(B) *Protection from malicious software*

Continued on Next Page

Security 11.0 Contingency Plan, Disaster Recovery

FULL POLICY LANGUAGE:

Policy Purpose:

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

Policy Description:

1. The **organization** shall establish (and implement as needed) procedures for responding to an emergency or other occurrence (i.e., fire, vandalism, system failure, or natural disaster) that damages systems containing ePHI. These procedures consist of:
    a. Applications and data criticality analysis;
    b. Data Backup;
    c. Disaster Recovery Plan; and
    d. Emergency Mode Operation Plan.
2. Each of these procedures shall be evaluated and updated at least annually as business needs and technology requirements change.

Applications and Data Criticality Analysis:

1. The **organization** shall assess the relative criticality of its specific applications and data for purposes of developing its Data Backup Plan, its Disaster Recovery Plan, and its Emergency Mode Operation Plan.
2. The **organization** shall identify critical business functions, define impact scenarios, and determine resources needed to recover from each impact.
3. The assessment of data and application criticality shall be conducted periodically and at least annually to ensure that appropriate procedures are in place for data and applications at each level of risk.

Data Backup Plan:

1. All ePHI shall be stored on network servers in order for it to be automatically backed up by the system.
2. ePHI may not be saved on the local drives of personal computers.
3. ePHI stored on portable media (i.e., thumb drives, external hard drive, CD ROM Disks) shall be saved to the network to ensure backup of ePHI data.
4. The **organization** shall conduct daily backups of user-level and system-level information and store the backup information in a secure location. A weekly backup shall be stored offsite.
5. The **organization** shall establish and implement a Data Backup Plan, pursuant to which it will create and maintain retrievable exact copies of all ePHI.
6. The Data Backup Plan shall apply to all files that may contain ePHI.

7. The Data Backup Plan shall require that all media used for backing up ePHI be stored in a physically secure environment, such as a secure, off-site storage facility. Or, if backup media remains on site, the media shall be stored in a physically secure location, different from the location of the computer systems it usually backs up.
8. If a **non-organization**, off-site storage facility or backup service is used, a written contract shall be entered into, to ensure that the contractor shall safeguard the ePHI in an appropriate manner.
9. Data backup procedures outlined in the Data Backup Plan shall be tested on at least an annual basis, to ensure that exact copies of ePHI can be retrieved and made available.
10. The **organization** shall submit its new and revised Data Backup Plan to the Chief Compliance Officer for approval.

Disaster Recovery Plan:

1. To ensure that the **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, the **organization** shall establish and implement a Disaster Recovery Plan. The Disaster Recovery Plan shall provide procedures for restoration or recovery of any loss of ePHI, and shall indicate the systems needed to make that ePHI available in a timely manner. The Disaster Recovery Plan for the **organization** shall be incorporated into the **organization's** Disaster Recovery Plan.
2. The Disaster Recovery Plan shall include procedures to restore ePHI from data backups in the case of a disaster causing data loss.
3. The Disaster Recovery Plan shall include procedures to log system outages, failures, and data loss to critical systems. In addition, procedures will be implemented to train the appropriate personnel on the Disaster Recovery Plan.
4. The Disaster Recovery Plan shall be documented and easily available to the necessary personnel at all times. These personnel shall be trained to implement the Disaster Recovery Plan.
5. The disaster recovery procedures outlined in the Disaster Recovery Plan shall be tested on a periodic basis to ensure that ePHI and the systems needed to make ePHI available can be restored or recovered.
    a. The **organization** shall submit its new and revised Disaster Recovery Plan to the Chief Compliance Officer for approval.

Disaster and Emergency Mode for Small Practices:

Small businesses shall maintain a list of persons/departments to call, along with their phone numbers. The list shall contain at least the following persons/departments, along with their phone numbers:

1. Real Estate/Office Suite Maintenance/Management;

2. Computers;
3. Computer Networking;
4. Restoration of Data to Server or Connection to the Internet;
5. EHR Support; and
6. Any other person or department needed to continue business.

Emergency Mode Operation Plan:

1. The **organization** shall establish and implement, as needed, procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode. Emergency mode operation involves critical business processes that shall occur to protect the security of ePHI during and immediately after a crisis situation.
2. Emergency mode operation procedures outlined in the Disaster Recovery Plan shall be tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode.
3. The **organization** shall submit its new and revised Emergency Mode Operation Plan to the Chief Compliance Officer for approval.

Policy Responsibilities:

The Chief Compliance Officer shall oversee the creation, evaluation, testing, and updating of the various contingency plans described herein.

The **organization** shall submit its new and/or revised procedures and plans to the Security Officer for approval and ongoing evaluation. Any procedures developed by the **organization** shall be consistent with its HIPAA policies and not deviate from the **organization's** standards.

For additional information on the terms used in this policy, please click here.

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 12.0 Business Associates

FULL POLICY LANGUAGE

Policy Purpose:

To provide rules for determination of what contractors of **organization** are Business Associates, and to provide rules for creation, review, and termination of Business Associate Agreements.

Policy Description:

Business Associates:

1. The **organization** has many contractual and business relationships. However, not all contractors or business partners are "Business Associates," as that term is defined by HIPAA. This security policy only applies to contractors or business partners that fall within the definition of a "Business Associate." Essentially (and as explained in greater detail under "Definitions," below), a Business Associate is any person or organization that the **organization** hires to help the **organization** to do something. The "something" under the contract involves the **organization's** either directly or indirectly sharing protected health information (PHI) or electronic protected health information (ePHI) with the Business Associate.
2. The Lead Compliance Officer(s) of the **organization** shall review all contracts to determine if the contract requires a Business Associate Agreement ("BAA"). If a BAA is required, contract managers must complete the BAA and notify the Compliance Officer(s). The BAA requires the Business Associate to provide satisfactory assurance that the Business Associate shall appropriately safeguard PHI and ePHI, and report any security incidents.
3. The **organization** shall audit the Business Associate via electronic questionnaire. If decided by the Chief Compliance Officer, the **organization** shall conduct a security audit of the Business Associate's HIPAA Policies and Procedures as a means of due diligence to ensure that the Business Associate 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 the **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, the **organization** shall, 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, the **organization shall** terminate the contract or arrangement, if feasible. If termination is not feasible, the problem shall be reported to the Office for Civil Rights (OCR) within 30 days of the incident.

Policy Responsibilities:

The Chief Compliance Officer, the Security Officer, and the Privacy Officer of the **organization** shall work together to ensure that all Business Associates are identified, tracked, and investigated when an allegation is made.

Procedures:

Tracking and Identifying Company Business Associates:

The **organization** shall identify those business relationships that meet the definition of a Business Associate relationship. Contract managers shall note that designation in the contract record, and notify the Chief Compliance Officer when a contractor is determined to be a Business Associate.

Response to Complaints about Business Associates:

A workforce member of the **organization** may receive a report or complaint, from any source, about the Business Associate's inappropriately or inadequately, safeguarding PHI. If and when a workforce member receives a report or complaint, the workforce member shall promptly provide information regarding that report or complaint to the Chief Compliance Officer(s). The Chief Compliance Officer(s) shall coordinate with the Business Associate's contract administrator to document the alleged violation, and determine if remediation is required for the Business Associate to attain/retain contract compliance.

Where contract compliance cannot be attained/retained, **the organization shall terminate the contract, if feasible**. If termination is not feasible, the Chief Compliance Officer shall report the problem to the Office for Civil Rights (OCR) within 30 days of the incident.

RELEVANT HIPAA REGULATIONS:

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

Continued on Next Page

Security 13.0 Monitoring and Effectiveness

FULL POLICY LANGUAGE:

Policy Purpose:

The intent of this policy is to establish periodic evaluations of the **organization's** policies and procedures, to ensure these measures detect, contain, and correct security violations. The evaluation shall determine whether the HIPAA policies and procedures are effectively safeguarding the confidentiality, integrity, and availability of ePHI. Security assessments shall be conducted periodically to determine continued compliance with security standards and specifications. Assessments are conducted 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.

Policy Description:

Risk Assessment & Management:

The **organization**, along with the Security Officer, shall monitor the effectiveness of its ability to secure ePHI. In order to accomplish this, the **organization** shall conduct a risk assessment 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 the **organization** are added;
5. Security breaches are identified; and
6. Changes in the mode or manner of service delivery are made.

As part of risk management, security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level shall be documented and implemented.

Risk Management Control:

The primary goal of risk management is to facilitate communications and coordinate all changes that may occur in the IT environment. These changes include, but are not limited to, the installation, update, or removal of network services and components, operating system upgrades, applications, database servers, or software.

Change Notification:

1. For informational purposes, the Chief Compliance Officer and the Security Officer shall be notified, by email, of changes. Notification shall be given within 48 hours of the change.
2. Emergency Changes shall be communicated to the Chief Compliance Officer and the Security Officer as soon as is reasonable.
3. Any change with a negative effect that could adversely affect customers, patients, or clients, shall be communicated to the Chief Compliance Officer and the Security Officer as soon as is reasonable.

Change Implementation:
All non-emergency changes made as part of risk management, shall occur within the recognized downtime unless approved in advance by all affected parties. Interdepartmental non-emergency changes shall occur as per the dictates of department procedures.

Change Closure:
When **organization**, under its risk management policy and procedure, completes a change or closes a change, that change or close shall be documented.

Evaluation:
The **organization** shall conduct an assessment of security controls at least annually. The assessment shall be conducted to determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome.

Technical and non-technical evaluations shall be conducted periodically to identify any new risks or to determine the effectiveness of the HIPAA Security Policies and Procedures. These evaluations include, but are not limited to, the following:

1. Random audit reviews of a facility's physical environment security;
2. Random audit reviews of workstation security;
3. Periodic, unannounced tests of the physical, technical, and administrative controls;
4. Assessment of changes in the environment or business process that may affect the HIPAA Security Policies and Procedures;
5. Assessment when new federal, state, or local laws and regulations, that may affect the HIPAA Security Policies and Procedures; are implemented;
6. Assessment of the effectiveness of the HIPAA Security Policies and Procedures when security violations, breaches or other security incidents occur; and
7. Assessment of redundancy needed in the network or servers for ePHI availability.

Policy Responsibilities:
The Chief Compliance Officer:

1. The Chief Compliance Officer must coordinate with the Security Officer(s) to conduct audits of compliance with the HIPAA Security Rule;
2. Shall coordinate the creation of procedures to implement this policy; and
3. Shall have responsibility for providing tools and processes for assessing technical and nontechnical evaluations as part of the **organization's** ongoing compliance efforts.

If assessments recommend changes to the HIPAA Policies and Procedures, the Chief Compliance Officer is responsible for reviewing these changes and presenting them to management. If needed, the Chief Compliance Officer will update the workforce training materials.

Procedures:

The Chief Compliance Officer shall create procedures to ensure ongoing evaluations and assessments are completed to mitigate risks to ePHI.

Risk Management: Risk management is an information security process. This process requires an **organization** to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the general requirements of the HIPAA Security Rule.

RELEVANT HIPAA REGULATIONS:

- §164.308(a)(8) *Perform a periodic technical and non-technical evaluation*
- §164.308(a)(1)(i) *Security management process*
- §164.308(a)(1)(ii)(A) *Risk analysis*
- §164.308(a)(1)(ii)(B) *Risk management*

Continued on Next Page

Security 14.0 Security Awareness and Training

FULL POLICY LANGUAGE:

Policy Purpose:

To provide rules for training of workforce and management on system and application security awareness principles.

Policy Description:

Security Awareness Training:

Security awareness training is key to eliminating the **organization's** exposure to both malicious threats and accidental errors or omissions.

System & Application Training:

This policy sets forth a minimum standard for system and application security awareness to reduce the **organization's** risk. The standard contains the following components:

1. Proper uses and disclosures of the ePHI stored in the application;
2. How to properly log on and log off the application;
3. Protocols for correcting user errors;
4. Instructions for contacting a designated person or help desk when ePHI may have been altered or destroyed in error; and
5. Reporting a potential security breach.

HIPAA Security Training:

1. All **organization** workforce members shall receive security training. The Chief Compliance Officer, or the Security Officer under the Chief Compliance Officer's management, will provide the training and training materials.
    a. Worker-Level Training: This training covers Security Policies and Procedures that directly affect members of the workforce.
    b. Managerial-Supervisory Training: This training encompasses all HIPAA Security Policies and Procedures, as well as Management's role in enforcement and supervision.
2. All new workforce members are required to attend the appropriate training within sixty (60) days of entering the workforce.
3. All workforce members must receive training annually.

Tracking Security Training:

The **organization's** training coordinator or designee shall enter their workforce members into The Guard, to sign them up for the appropriate level of training.

HIPAA Security Reminders:

The Chief Compliance Officer and Security Officer shall develop and implement periodic security updates and issue at least quarterly reminders to the **organization's** workforce. These security reminders shall be provided using those media that the **organization** uses to communicate with its workforce (i.e., email, posters, newsletters, intranet site, etc.).

Policy Responsibilities:

1. Security Officers are responsible for ensuring that all workforce members in their operational areas are trained no later than thirty (30) days after entering their workforce.
2. Chief Compliance Officers shall have oversight responsibility to audit reports from The Guard to ensure required workforce member attendance.
3. If needed, the Chief Compliance Officer or Security Officer may require workforce members to attend more training if security incidents warrant such further training.

Procedures:

1. The **organization** shall create and maintain written procedures on how new workers are notified of training, when training takes place, and where new workers should report for training.
2. The **organization** shall submit any new and/or revised procedures and plans to the Security Officer and Chief Compliance Officer for approval and ongoing evaluation. All procedures developed by the **organization** shall be consistent with its HIPAA policies and will not deviate from the **organization's** existing privacy and security standards.

RELEVANT HIPAA REGULATIONS:

- § 164.308(a)(5)(i) *Security awareness and training*
- § 164.308(a)(5)(ii)(A) *Security reminders*

Continued on Next Page

Security 15.0 Sanction Policy

FULL POLICY LANGUAGE:

Policy Purpose:

To outline disciplinary measures (sanctions) to be taken against members of the workforce who violate the HIPAA Security Rule and/or **organization's** Security Rule policies and procedures as set forth in this manual.

Policy Description:

Sanctions:

1. All members of the **organization's** workforce must be aware of their responsibilities under the **organization's** HIPAA Security Rule policies and procedures.
2. All members of the **organization's** workforce must sign a HIPAA Confidentiality form, indicating that they have been informed of the **organization's** security practices.
3. Managers and supervisors must ensure that workforce members who have access to ePHI are informed of their responsibilities with respect to that ePHI.
4. Management must ensure that training is timely and appropriate; that updates are timely communicated to workforce members; and that only the most current, up-to-date information is used in training, policies, and procedures.
5. Members of the **organization's** workforce, who violate policies and procedures relating to safeguarding of protected health information or otherwise confidential information, are subject to disciplinary action by the **organization.** Disciplinary action may include measures up to and including immediate dismissal from employment.
6. Corrective action for violations, including, but not limited to, contract cancellation or termination of services, shall be implemented by the **organization** and shall apply to members of the workforce not subject to the **organization's** discipline process.
7. Members of the workforce who knowingly and willfully violate state or federal law for failure to safeguard ePHI are subject to criminal investigation and prosecution, and/or civil monetary penalties.
8. If the **organization** fails to enforce security safeguards, it may be subject to administrative penalties by the Office for Civil Rights (OCR), including federal funding penalties.

Reporting Violations:

All workforce members shall notify the Security Officer and Chief Compliance Officer when there is a reasonable belief that any security policies or procedures are being violated.

Retaliation Prohibited:

1. Neither the **organization** as an entity nor any member of its workforce shall intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any individual for:
    a. Exercising any right established under the **organization's** policy;
    b. Participating in any process established under the **organization's** policy including the filing of a complaint with the **organization** or with the Office for Civil Rights;
    c. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing relating to the **organization's** policy and procedures; and
    d. Opposing any unlawful act or practice, provided that the individual or other person (including a member of the **organization's** workforce) has a good faith belief that the act or practice being opposed is unlawful and the manner of such opposition is reasonable and does not involve a use or disclosure of an individual's protected confidential information in violation of the **organization's** policy.
2. Those engaging in retaliation shall be subject to the sanctions under this policy.

Policy Responsibilities:
All workforce members are responsible for notifying the Security Officer and Chief Compliance Officer when there is a belief that any security policies are being violated.

Workforce: The definition of the **organization's** workforce is taken from the HIPAA Privacy Rule. Section 160.103 of the Privacy Rule defines the term "workforce" as "Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Covered Entity, is under the direct control of such entity, whether or not they are paid by the Covered Entity."

RELEVANT HIPAA REGULATIONS:

- § 164.308(a)(1)(ii)(C) *Sanction policy*

Security 16.0 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:

1. The Compliance Officers (Chief Compliance Officer and/or Security Officer) shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rule. The Compliance Officers shall work with workforce members to draft and revise policies and procedures.
2. All policies and procedures implemented to comply with the HIPAA Security Rule shall be documented in writing (which may be in electronic form). All records of actions, activities, or assessments required by the Rule shall be documented. The documentation shall be detailed enough to communicate the security measures taken and to facilitate periodic evaluations.
3. 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.
4. All documentation shall be available to those persons responsible for implementing the procedures to which the documentation pertains.
5. Documentation shall be reviewed at least annually, and updated as needed, in response to environmental or operational changes affecting the security of the ePHI.

Policy Responsibilities:

Compliance Officers:

The Compliance Officers shall be responsible for leading the development, implementation, and maintenance of the policies, procedures, and related documentation.

Department Management:

The **organization** shall submit all new and revised procedures to the Compliance Officers for approval and ongoing evaluation.

Procedures:

In general, the following process shall be used to develop and implement policies and procedures:

1. The Compliance Officers shall draft new or updated HIPAA information security policies;

2. The new information security policy shall be presented to the **organization's** management for awareness, input, and endorsement;
3. The Compliance Officers shall give final approval for the new or updated policy; and
4. The Compliance Officers shall communicate the new or updated policy to the workforce including updating training and related materials as needed.

Any procedures developed by the **organization** shall be consistent with its HIPAA policies, and shall not deviate from **organization's** existing privacy and security standards.

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*

Continued on Next Page

Security 17.0 Satellite Office and Home Office Policy

FULL POLICY LANGUAGE:

Policy Purpose:

The intent of this policy is to specify the circumstances under which devices can be used at Satellite Office and Home Office sites. These sites, by definition, contain no signage to designate that they are part of, or perform services for, the main healthcare entity. These locations are used solely for treatment purposes. When treatment is finished, the provider leaves the facility. Satellite Offices and Home Offices may not be used for storing PHI documented in physical or digital form.

Policy Description:

1. Devices used at Satellite and Home sites must be protected and encrypted and listed in the Device Audit as encrypted.
2. Site(s) must have a Physical Site Audit filled out and stored in The Guard.
3. All **organization** staff that work in the Satellite and Home offices must go through HIPAA training.
4. No footprint (evidence of PHI) shall be allowed at either Satellite or Home Offices.
5. If the above are not followed, the **organization** must be able to defend its decisions to the Department of Health and Human Services (HHS), should a breach occur because these protocols were not followed.

Policy Responsibilities:

The Chief Compliance Officer shall oversee the creation, approval, and updating of the Satellite Office and Home Office Policy. New and/or revised procedures and plans shall be submitted to the Security Officer for approval and ongoing evaluation.

Procedures:

The **organization** shall submit its new and/or revised procedures and plans to the Security Officer for approval and ongoing evaluation. Any procedures developed by the **organization** shall be consistent with its HIPAA policies and not deviate from the **organization's** existing privacy and security standards.

If any of the above does not apply to an office, then this site is considered a location and is subject to all the HIPAA requirements that the main office is subject to.

Example of a Satellite Office:

A doctor's office in city A has a lot of patients in city B, so, once a week, the doctor uses a site in city B (i.e., an examination room in another doctor's office, etc.) to see patients who live there so they do not have to travel as far. This site is not used for storing charts, for storing computers, or for leaving any documentation behind. It is strictly used for seeing the doctor's patients, and then the site is vacated. When leaving, the doctor leaves behind

no footprint, no computers, no charts, no trash, and nothing about or pertaining to any of the patients that were there that day.

Home Office: A home office is a location with no signage to designate that it is part of, or performs services for, the main **organization**. This location is not used for storing charts, for storing computers, and does not retain any documentation. It is strictly used for providing treatment and healthcare viewing of electronic records. There is no footprint, no data stored on computers, no charts, no trash, nothing that can be traced back to any of the PHI that was interacted with. If the **organization** uses a home office, the **organization** should not allow storage of PHI at the Home Office. Printed matter should be shredded immediately after use, and it should not be stored. Computers should be set up so PHI cannot be downloaded from the main site. **No footprint can be left at the home office.**

If any of the above does not apply, then this site is not considered to be a Home Office. Instead, it is considered to be a location and is subject to all the HIPAA requirements that the main office is subject to.

Continued on Next Page

Security 18.0 Work from Home Policy

FULL POLICY LANGUAGE:

Policy Purpose:

This policy outlines the security procedures to be followed by employees who telecommute.

Policy Description:

Telecommuting is a voluntary work arrangement that allows employees to perform their jobs at home as part of the regular workweek. Employees who telecommute must observe proper security procedures.

Procedures:

Employees who telecommute must take proper security measures to ensure that ePHI remains appropriately safeguarded. With respect to the devices employees who telecommute use to perform their work, employees must do the following:

1. Employees must have a device that the employee will dedicate for business purposes only.
2. Employees must ensure device drives are encrypted. This can be accomplished by using an encryption application such as Microsoft BitLocker (requires Windows 10 Pro) or Apple File Vault.
3. Employees must install antivirus and antimalware protections before employees can use a device for business purposes.
4. Employees must enable the "Automatic Updates" function of any device, software program, or operating system used to perform work.
5. Employees must have a strong password-protected account on their device. Password guidelines, which incorporate best practices from the latest National Institute of Standards and Technology (NIST) guidelines (set forth in NIST SP 800-63B) are set forth below, and shall be used by employees:
    a. Passwords shall be a minimum of eight (8) characters in length. A maximum length of 64 characters is permitted.
    b. Passwords may consist of all special characters; however, use of all special characters is not a requirement.
    c. Password use shall be restricted as follows:
        i. Use of sequential and repetitive characters (i.e., 12345 or aaaaa) is restricted.
        ii. Context-specific passwords (i.e., the name of organization's website) are restricted.
        iii. Commonly-used passwords (i.e., p@ssw0rd, etc.) shall be restricted.
        iv. Passwords obtained from previous security breaches shall not be used.

6. Employees must have a password-protected screen lock timeout set to a maximum of 15 minutes.
7. Employees must ensure that all wireless router traffic is encrypted, using (at a minimum) WPA2-AES encryption.
8. Employees must make sure that the password to a wireless network is a strong password, in accordance with (5) above.
9. Employees may not download or print PHI at home offices or any other location from which employees telecommute.
10. Employees must conduct a physical site audit, and provide the details of that audit, to the current Security Officer, no less than once every twelve months. The audit consists of the following questions:
    a. Does the employee store paper documents that contain PHI in the employee's home office?
    b. Does the employee print paper documents that contain protected health information at the employee's home office?
    c. Does the employee receive paper faxes at a physical fax machine in the employee's home office?
    d. Does the employee take paper or electronic files containing PHI or ePHI to the employee's home office?
    e. Does the employee's home office have a lockable door?
    f. Does the employee's home or home office have an alarm system?
11. **Organization's** Security Officer shall conduct its own portion of the physical site audit referenced in (10). The physical site audit for the Security Officer consists of the following questions:
    a. Is the drive on the employee's computer encrypted using either Apple File Vault or Microsoft BitLocker encryption?
    b. Does the employee's computer have antivirus and antimalware software installed, and is the software up-to-date?
    c. Are automatic updates on employee devices, operating systems, and applications turned on?
    d. Is the employee's computer protected with a "strong password," as that phrase is defined in (5), above?
    e. Is the employee's computer set to lock after 15 minutes of inactivity?
    f. If the employee has a wireless router, is the router protected with WPA2-AES encryption?
    g. If the employee has a router, is the router protected with a strong password.
12. **Organization's** Security Officer and/or IT department must confirm employees have all security measures required by this policy in place, before access to organization's resources is granted.

Security 19.0 Bring Your Own Device Policy

FULL POLICY LANGUAGE:

Policy Purpose:

To outline the security precautions that must be taken by employees who conduct work using their personally-owned devices.

Policy Description:

Organization may allow employees to conduct work using their personally-owned devices (such as smartphones, laptops, and PDAs). When employees use their personally owned devices to access **organization's** resources and services, employees must take proper security precautions, so the security of both the devices and **organization's** data and technology infrastructure is maintained.

Procedures:

Expectation of Privacy:

Organization shall respect the privacy of employees' personal devices, and will only request access to these devices:

1. When required for IT personnel to implement security controls and measures; and
2. To respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings.

Acceptable Use:

1. Personal devices may be used for an "acceptable business use." "Acceptable business use" means use for activities that directly or indirectly support the **organization's** business functions.
2. Personal devices may be used for an "acceptable personal use" while on company time. "Acceptable personal use" means reasonable and limited personal communication or recreational activities, such as reading.
3. **Organization** has a zero-tolerance policy for texting or emailing while driving, Only hands-free talking while driving is permitted.
4. Personally-owned devices may never be used to:
    a. Store or transmit illicit materials.
    b. Store or transmit proprietary information.
    c. Harass others.
    d. Engage in outside business activities.
5. Employees may use their personally-owned devices to access, as necessary, the following company-owned resources: Email, Calendars, Contacts, and Documents.

Devices and Support:

- The following devices are supported:
    - iPhone, iPad, Android, Blackberry, Windows, Mac
- Connectivity issues are supported by IT; employees should contact the device manufacturer or their carrier for an operating system or hardware-related issue.
- Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software, and security tools, before they can access the network.

Security:

- Devices must be password-protected using a strong password.
- All devices must be encrypted according to NIST guidelines.
- The device must lock itself with a password or PIN if the device is idle for five minutes.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- Laptops, Smartphones, and tablets that are not on the company's list of supported devices are not allowed to connect to the network.
- Laptops, Smartphones, and tablets belonging to employees that are for personal use only are not allowed to connect to the network.
- Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.
- The employee's device may be remotely wiped if:
    - The device is lost or stolen.
    - The employee terminates his or her employment.
    - IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

Employee Responsibilities:

- While **organization** will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- The organization reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to the **organization** within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is expected to use his or her devices in an ethical manner at all times, and adhere to the company's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash,

errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

- The **organization** reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

Continued on Next Page

Glossary

Access Control: Control of the ability or the means necessary to read, write, modify, or communicate ePHI.

Audit Logs: Records of events based on applications, users, and systems.

Business Associate: Any entity that uses or discloses protected health information (PHI) on behalf of a Covered Entity (i.e. group health plan, hospital, etc.). Furthermore, a Business Associate is any person or organization that, on behalf of a Covered Entity, performs (or assists in the performance of) a function or activity involving the use or disclosure of PHI.

Business Associate Agreement/Business Associate Contract: A business associate agreement/business associate contract is a contract or other written arrangement, enforceable by law, between the covered entity and the business associate. The contract must be entered into before the business associate can create, receive, or transmit any PHI. In addition, the contract must (among other things):

- Describe the permitted and required uses of protected health information by the business associate;
- Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law; and
- Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.

Optimally, such contracts should be drafted as to apportion liability to where it properly is placed. Optimally, contracts should contain provisions to the effect that a covered entity is liable under the law for its breach (if any) of unsecured protected health information, and that the business associate is liable under the law for its breach (if any) of unsecured protected health information.

Business Associate Functions and Activities Include: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. Business associate services are legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

Chief or Lead Compliance Officer: The individual designated by **organization** as being in charge of overall privacy and security compliance for the organization. The Chief

Compliance Officer is the only individual within organization who can resolve a security incident.

Confidentiality Agreement: An agreement between a healthcare organization and a vendor, or an agreement between a healthcare organization and a member of its staff. The agreement requires that any organization hired to perform a task, or any organization employee, who accidentally encounters ePHI, to keep such ePHI confidential.

Covered Entity: A health plan or a health care provider that stores or transmits any health information in electronic form in connection with a HIPAA covered transaction.

Critical Business Functions: Critical business processes that are needed for protection of the security of electronic protected health information.

Decryption Key: Computer code required to transform (decrypt) an encrypted message, document, or other data into a form that can be freely read.

Degaussing: The process of demagnetizing data. Once a hard drive is degaussed, it cannot be read again.

Encryption: Under the HIPAA Security Rule, encryption is defined as "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.

Encryption Key: A random string of bits (tiny pieces of information, represented as numbers) generated specifically to scramble and unscramble data. Encryption keys are created with algorithms designed to ensure that each key is unique and unpredictable.

ePHI: Electronic/Protected health information means individually identifiable health information that is:

- Transmitted by electronic media;
- Maintained in electronic media; or
- Transmitted or maintained in any other form or medium.

Extranet: A controlled private network that allows access to specific entities (i.e., partners, vendors, or suppliers). Extranet access is limited to a subset of the information accessible from an organization's intranet.

HIPAA Security Rule: The HIPAA Security Rule requires healthcare organizations to protect patients' electronically stored, protected health information (known as "ePHI") by using appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of this information.

Intranet: An **intranet** is a private network that can only be accessed by authorized users. An **intranet** is designed for internal communications within **organization**.

LAN: Stands for Local Area Network. A Local Area Network is a computer network that links devices within a building or group of adjacent buildings.

Malware: Malware is short for "malicious software." Malware consists of programs designed to damage computer systems. Malware consists of (among other things) viruses, worms, trojan horses, and spyware.

Network Closet: A **closet** or a small room where electrical **wiring** and computer **networking** hardware is installed.

Paper PHI: Protected health information that is not in an electronic format.

Risk Analysis: Risk analysis is the assessment of the risks and vulnerabilities that could negatively impact the confidentiality, integrity, and availability of the electronic protected health information (ePHI) held by a covered entity, and the likelihood of occurrence. A risk analysis may include taking inventory of all systems and applications that are used to access and house data, and classifying them by level of risk. A thorough and accurate risk analysis considers all relevant losses that would be expected if the security measures were not in place, including loss or damage of data, corrupted data systems, and anticipated ramifications of such losses or damage.

Risk Management: Risk management is an information security process. This process requires an **organization** to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the general requirements of the HIPAA Security Rule.

Satellite Office: A Satellite Office is a non-descript location, with no signage to designate that it is part of, or performs services for, the main **organization**. This location is used only for providing treatment. When treatment is finished, the individual leaves. The Satellite Office is not used for storing PHI documented in physical or digital form. When leaving the Satellite Office, no footprint, computers, charts, or trash can be left behind. Nothing can be traced back to any of the PHI that was interacted with.

Security Breach: The acquisition, access, use, or disclosure of protected health information in a manner not permitted, which compromises the security or privacy of the protected health information.

Security Incident: An attempt (whether successful or not) to do something unauthorized with respect to ePHI. The "something" that is unauthorized, is an unauthorized access, use, disclosure, modification, destruction, or interference.

Security Officer: A HIPAA security officer is responsible for the continuous management of information security policies, procedures, and technical systems in order to maintain the confidentiality, integrity, and availability of ePHI.

Security Rule Administrative Safeguards: These are safeguards that have to do with internal policies and procedures and proper employee training. Documented security policies and procedures create a uniform process that staff members can follow to maintain the security of ePHI. By implementing administrative safeguards, you can mitigate the potential for a security breach relating to human error.

Security Rule Confidentiality, Integrity, and Availability (CIA) of ePHI: The Security Rule defines "confidentiality" to mean that ePHI is not available or disclosed to unauthorized persons. Under the Security Rule, "integrity" means that ePHI is not altered or destroyed in an unauthorized manner. "Availability" means that ePHI is accessible and usable on demand by an authorized person.

Security Rule Physical Safeguards: These are safeguards that protect **organization's** physical premises and infrastructure, to ensure there is no unauthorized ePHI access.

Security Rule Technical Safeguards: These are safeguards that include network security and data security. Technical safeguards include measures **the organization** can take to reduce the risk of a cybersecurity incident, especially relating to improper transmission of ePHI over email or malware.

System Administrator: An individual responsible for managing the operation of a computer system.

Training: The HIPAA Security Rule requires **organization** to provide **workforce training and management.** To comply with this requirement, organization shall at all times provide for appropriate authorization and supervision of workforce members who work with ePHI. **Organization** shall train all workforce members regarding its security policies and procedures. **Organization** shall implement and apply appropriate sanctions against workforce members who violate its policies and procedures.

Virus: A virus is a piece of computer code that inserts itself within the code of another standalone program, then forces that program to take malicious action and spread itself.

VPN: Virtual Private Network. A VPN is an encrypted internet connection that allows users to safely transmit sensitive data, preventing unauthorized user access.

WAN: Stands for Wide Area Network. A Wide Area Network is a computer network in which the computers connected may be far apart (i.e., half a mile or more).

WLAN: Stands for Wireless Local Area Network. A wireless LAN is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area, such as a home, campus, or office building.

Workforce: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Worm: A worm is a standalone piece of malicious software that reproduces itself and spreads from computer to computer.