HIPAA Security To Do List

© Copyright 2002-2015 by HIPAATraining.com All rights reserved. No part of the "HIPAA Security Documentation Kit" may be reproduced or transmitted in any form by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written consent of HIPAATraining.com.

HIPAATraining.com Disclaimer Notice

Please read the following disclaimer if you intend to use HIPAATraining.com's HIPAA Security Documentation Kit.

"HIPAA Security Documentation Kit" was created and designed to provide healthcare providers, mental health providers, employer group health plans, health insurance providers, and business associates with a comprehensive, concise, and easy-to-use resource for implementing HIPAA Security. The information provided here is intended for educational and reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by HIPAATraining.com The information is based on current federal law and subject to change based on changes in federal law or subsequent interpretative guidance. In addition, the information is based on federal law and must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. All material must be viewed in the context of your own organization and environment. Legal opinions or decision documentation may be needed to apply/interpret it.

While "HIPAA Security Documentation Kit" is believed to be generally accurate as of the date of its last revision in 2015, HIPAATraining.com neither guarantees nor warrants the accuracy of the content in "HIPAA Security Documentation Kit". You should be aware that the HIPAA rules may change in the future. "HIPAA Security Documentation Kit" should not be used as a substitute for professional legal or other advice. You use or rely on the information and material in "HIPAA Security Documentation Kit" at your own risk.

© Copyright 2002-2015 by HIPAATraining.com All rights reserved. No part of "HIPAA Security Documentation Kit" may be reproduced or transmitted in any form by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written consent of HIPAATraining.com.

Step 1. Understanding HIPAA Security

INTRODUCTION

Before you begin implementing HIPAA Security, you will need to learn about it and understand how it will impact your organization. You will also need to designate an individual to be the HIPAA Security Compliance Officer. They will be responsible for implementing HIPAA Security at your organization and they will be the designated point person for HIPAA Security issues at your organization. While this the HIPAA Privacy compliance officer and the HIPAA Security compliance officer can be two different individuals, for most organizations it is easier to have the same individual handle both and as such be the over HIPAA compliance officer for the organization. The assumption is that if you are reading this, this means you as you have been "volunteered" as the HIPAA Security Compliance Officer.

ACTION ITEMS

☑ **1. Designate an individual to serve as the HIPAA Security Compliance Officer.**

HIPAA Security Compliance Officer's Name: Sean Baumgartner

This person will be responsible for implementing HIPAA Security at your organization and will be the focal point for all HIPAA Security related issues for your organization. Note that the HIPAA Security Compliance Officer is a designated position required by the HIPAA Security standards and will be revisited in later steps. The person listed here should be the one going through this kit.

☑ **2. Take and complete HIPAA Security training.**

As one of the key persons responsible for the HIPAA Security implementation, it is critical that you learn and understand HIPAA Security and HIPAA requirements overall so that you can get the big picture of the overall implementation effort. The training course, "HIPAA Security Training", is located in your registered HIPAATraining.com account and can be selected from the red Product Selector button on the left.

☐ **3. Have your IT staff and others who will be involved with the HIPAA Security implementation take and complete HIPAA Security training.**

In addition to yourself, you want any staff members who will be helping you with the HIPAA Security implementation to also take the training. This most often is members of the IT staff or an external IT consultant. The training course, "HIPAA Security Training", is located in your registered HIPAATraining.com account and can be selected from the red Product Selector button on the left.

☑ **4. Review Frequently Asked Questions for additional information.**

Once you have completed the training, you are likely to still have questions. You can review the list of Frequently Asked Questions, located under the reference section of your HIPAA Training.com account for some of the most common questions. You can also visit HHS's online FAQS at: http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html. For all questions that remain, feel free and contact HIPAATraining.com at 512-402-5963 or by email at support@hipaatraining.com.

Template: Reference → HIPAA Frequently Asked Questions

© Copyright 2002-2015, HIPAATraining.com

☐ **5. HIPAA Privacy Compliance.**

If your organization has not already done so, then you should also make sure that your organization is compliant with the HIPAA Privacy regulations. HIPAA Privacy compliance is specifically about safeguarding protected health information in all its forms from improper use and disclosure whereas HIPAA Security is specifically about safeguards around protected health information in electronic form. HIPAATraining.com offers a similar kit to this HIPAA Security Documentation Kit called the HIPAA Privacy Documentation Kit.

© Copyright 2002-2015, HIPAATraining.com

Step 2. Administrative Safeguards

INTRODUCTION

The HIPAA Security Rule's requirements are organized into three categories:

Administrative safeguards	policies and procedures designed to show how the entity will comply with the security rule
Physical safeguards	the controlling of physical access to protect against inappropriate access to protected data
Technical safeguards	the controlling of access to computer systems and the protection of communications containing PHI transmitted electronically over open networks

The first of these three categories, Administrative safeguards, is the focus of this step.

The Administrative Safeguards are administrative actions, policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of the organization's workforce in relation to the protection of that information.

The Administrative safeguards consist of the following 9 standards:

- Assigned Security Responsibility
- Security Management Process
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts

NOTE: For employer group health plans, substitute group health plan name for all <organization name> placeholders in documents.

ACTION ITEMS

☑ **1. Assigned Security Responsibility (R)**

For the **Assigned Security Responsibility (R)** standard, the organization must designate a security official (one individual not an organization) to be responsible for the development and implementation of the policies and procedures and having overall responsibility for the security of the organization's ePHI (electronic protected health information).

HIPAA Security Compliance Officer's Name: Sean Baumgartner

The Security Officer may be a newly created job position or these duties may be added to an existing job description. The best candidate to be the Security Officer is many times the HIPAA Privacy Officer. It should not just automatically be someone from the IT department, because HIPAA Security is much more than a technical solution to providing protection to electronic health information.

Template: Administrative → Security Officer Job Description

© Copyright 2002-2015, HIPAATraining.com

☐ **2. Security Management Process**

The **Security Management Process** standard requires an organization to establish and implement policies and procedures to prevent, detect, contain and correct security violations. This standard consists of the following implementation specifications:

a. **Risk Analysis (R)**

Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.

Template: Administrative → HIPAA Security Risk Assessment

b. **Risk Management (R)**

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. This document will be a gap analysis of things you find that need to be fixed or implemented as you go through the various policies and procedures. Once you fix them, you will know your policies and procedures match your organization's safeguards.

Template: Administrative → Risk Management

c. **Sanction Policy (R)**

Apply appropriate sanctions against workforce members and business associates who fail to comply with security policies and procedures.

Create a sanction policy for the Security standards. These sanctions can be combined with the Privacy Rule sanctions. As with the Privacy Rule, the type and severity of the sanctions imposed, and for what causes, are determined by the organization. It is mandatory that this policy be documented, retained for six years, and should be periodically reassessed and updated as needed.

Template: Administrative → Policies and Procedures for Employee Sanction

In addition, the HIPAA Security officer should document each instance of workforce disciplinary action regarding security of ePHI in a written or electronic record. This documentation must be retained for six years from the date of its creation or the date when it was last in effect whichever is later.

Template: Administrative → Security Sanctions Log

d. **Information System Activity Review (R)**

Establish and implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident-tracking reports.

The organization will need to document what electronic PHI records will be reviewed and how often these records are reviewed to ensure there have been no security incidents that warrant attention. If the organization doesn't currently have access to reports or audit logs, the organization may want to ask its IT department or its software vendor to provide these reports. The access reports should also take into consideration security measures implemented to limit the access of a workforce member to electronic PHI. The procedures developed for this implementation need to be documented, retained for six years, and should be periodically reassessed and updated as needed.

Incorporated into: Technical → Policies and Procedures for Audit Control
Incorporated into: Administrative → Policies and Procedures for Security Incident Response and Reporting

© Copyright 2002-2015, HIPAATraining.com

☐ **3. Workforce Security**

The **Workforce Security** standard requires an organization to establish and implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information (ePHI) and includes the following implementation specifications:

Template: Administrative → Policies and Procedures for Workforce Security

a. **Authorization and/or Supervision (A)**

Establish and implement policies and procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed.

b. **Workforce Clearance Procedure (A)**

Establish and implement policies and procedures to determine if the access of a workforce member to ePHI is appropriate.

c. **Termination Procedures (A)**

Establish and implement policies and procedures for terminating access to ePHI when the employment of a workforce member ends or when the clearance procedures determine that a change in a worker's access privileges is appropriate.

☐ **4. Information Access Management**

The **Information Access Management** standard requires an organization to establish and implement policies and procedures for authorizing access to ePHI only when such access is appropriate based on the user's or recipient's role (role based access) and includes the following implementation specifications:

Template: Administrative → Policies and Procedures for Information Access Management

a. **Isolating Health care Clearinghouse Function (R)**

If a healthcare clearinghouse is part of a larger organization, it must take steps to protect its electronic PHI from unauthorized access by persons from that larger organization.

b. **Access Authorization (A)**

Establish and implement policies and procedures that specify levels of access for all personnel authorized to access ePHI

c. **Access Establishment and Modification (A)**

Establish and implement policies and procedures to specify how access to ePHI is granted and modified.

☑ **5. Security Awareness and Training**

The **Security Awareness and Training** standard requires an organization to train all members of their workforce on its security policies and procedures and includes the following implementation specifications:

Template: Administrative → Policies and Procedures for Security Awareness and Training
Template: Administrative → Log of HIPAA Security Training
Template: Administrative → Confidentiality Agreement

© Copyright 2002-2015, HIPAATraining.com

a. **Security Reminders (A)**

Provide periodic reminders to supplement initial security education.

b. **Protection from Malicious Software (A)**

Provide training on guarding against, detecting and reporting malicious software such as viruses and worms.

c. **Log-in Monitoring (A)**

Provide training on monitoring login attempts and reporting discrepancies.

d. **Password Management (A)**

Provide training on procedures for creating, changing, and safeguarding passwords.

☑ **6. Security Incident Procedures**

The **Security Incident Procedures** standard requires an organization to establish and implement policies and procedures to address security incidents (the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system) and includes the following single implementation specification:

a. **Response and Reporting (R)**

Develop a list of what constitutes a security incident in the context of the organization's operations. The organization will have to implement accurate and current security incident procedures for those items that have been identified as incidents. The procedures will need to include formal, documented report-and-response procedures. The security incident procedures relate to internal reporting of security incidents and do not specifically require the organization to report the incident to any outside entity, except if they are dependent upon business or legal considerations.

Template: Administrative → Policies and Procedures for Security Incident Response and Reporting

Develop a form to report and record the facts pertaining to any known or suspected violation of the HIPAA Security Rule standards or the laws and regulations governing the organization.

Template: Administrative → Security Incident Report

Develop a form to record the findings of an investigation pertaining to any known or suspected violation of the HIPAA Security Rule standards or the laws and regulations governing the organization.

Template: Administrative → Security Incident Investigation Form

☐ **7. Contingency Plan**

The **Contingency Plan** standard requires an organization to establish and implement policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI and includes the following implementation specifications:

Template: Administrative → Contingency Plan
Template: Administrative → Policies and Procedures for Contingency Planning
Template: Administrative → Contingency Plan Testing Schedule

© Copyright 2002-2015, HIPAATraining.com

a. **Data Backup Plan (R)**

Establish and implement policies and procedures to create and maintain retrievable exact copies of electronic PHI

b. **Disaster Recovery Plan (R)**

Establish and implement policies and procedures to restore any loss of data following a catastrophe.

c. **Emergency Mode Operation Plan (R)**

Establish and implement policies and procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode

d. **Testing and Revision Procedure (A)**

Establish and implement policies and procedures for periodic testing and revision of contingency plans. Take copies of the electronic protected information that have been backed up, restore it, and attempt to access it. Without testing the contingency plan, the organization would have no assurance that its critical data could survive an emergency situation. This testing should occur at least once a quarter and the results should be documented and retained for six years.

e. **Application and Data Criticality Analysis (A)**

Perform an analysis to assess the relative criticality of specific applications and data in support of other contingency plan components

☑ **8. Evaluation (R)**

The **Evaluation (R)** standard requires an organization to perform periodic technical and non-technical evaluations that determine the extent to which the organization meets the ongoing requirements of the Security Rule.

Template: Administrative → Policies and Procedures for Evaluation

An organization should:

- Verify adherence to the HIPAA Security Rule
- Verify that the necessary policies and procedures have been developed
- Verify that employees have been trained
- Verify that contingency plans are in place
- Verify that adequate access rights are in place
- Periodically evaluate computer systems and/or network design to ensure proper security has been applied

☐ **9. Business Associate Contracts and Other Arrangements**

The **Business Associate Contracts and Other Arrangements** standard requires an organization to develop and implement contracts that ensure that the vendors and subcontractors that create, receive, maintain, or transmit ePHI on the organization's behalf will appropriately safeguard the information and includes the following single implementation specification:

Template: Business Associate Contract & associated Policies and Procedures (included in HIPAA Privacy Documentation Kit)

© Copyright 2002-2015, HIPAATraining.com

a. **Written Contract or Other Arrangement (R)**

An organization is required to establish a contract (or other arrangement) that will appropriately safeguard PHI when it has to be shared with another organization

A Business Associate Contract is used between a Covered Entity and a Business Associate.

Template: Business Associate Contract & associated Policies and Procedures (included in HIPAA Privacy Documentation Kit)

The Subcontractor and Agent Contract is used between a Business Associate and any subcontractors or agents that it subsequently shares PHI with.

Template: Subcontrator and Agent Contract & associated Policies and Procedures (for Business Associates) (included in HIPAA Privacy Documentation Kit)

To simplify record keeping, an organization can also track vendors, business associates, and covered entities with whom the organization shares PHI in a Shared PHI List document. Utilize the appropriate version depending on if your organization is a covered entity or a business associate.

Template: Business Associate List (for Covered Entities) (included in HIPAA Privacy Documentation Kit)

Template: Shared PHI List (for Business Associates) (included in HIPAA Privacy Documentation Kit)

© Copyright 2002-2015, HIPAATraining.com

Step 3. Physical Safeguards

INTRODUCTION

The HIPAA Security Rule's requirements are organized into three categories:

Administrative safeguards	policies and procedures designed to show how the entity will comply with the security rule
Physical safeguards	the controlling of physical access to protect against inappropriate access to protected data
Technical safeguards	the controlling of access to computer systems and the protection of communications containing PHI transmitted electronically over open networks

The second of the HIPAA Security categories, Physical safeguards, is the focus of this step.

Physical safeguards are physical measures, policies and procedures to protect the organization's electronic information systems and related buildings and equipment, from natural and environmental hazards and unauthorized intrusion.

The Physical Safeguards consist of the following 4 standards:

- Facility Access Control
- Workstation Use
- Workstation Security
- Device and Media Controls

NOTE: For employer group health plans, substitute group health plan name for all <organization name> placeholders in documents.

ACTION ITEMS

☐ **1. Facility Access Controls**

The **Facility Access Controls** standard requires an organization to limit physical access to its facilities while ensuring that authorized access is allowed and includes the following implementation specifications:

Template: Physical → Policies and Procedures for Facility Access Controls
Template: Physical → Facility Repair Documentation Form

a. **Contingency Operations (A)**

Establish and implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

b. **Facility Security Plan (A)**

Establish and implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

c. **Access Control and Validation Procedures (A)**

© Copyright 2002-2015, HIPAATraining.com

Establish and implement policies and procedures that validate a person's physical access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

d. **Maintenance Records (A)**

Establish and implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security, for example maintenance to hardware, doors, locks and walls

☑ **2. Workstation Use (R)**

The **Workstation Use (R)** standard requires an organization to establish policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.

It is important to note that the term "workstation" means any electronic computing device, such as a desktop computer, laptop, PDA, etc.

Template: Physical → Policies and Procedures for Workstation Use

☑ **3. Workstation Security (R)**

The **Workstation Use (R)** standard requires an organization to implement physical safeguards for all workstations that can access ePHI in order to restrict access to authorized users.

It is important to note that the term "workstation" means any electronic computing device, such as a desktop computer, laptop, PDA, etc.

Template: Physical → Policies and Procedures for Workstation Security

☐ **4. Device and Media Controls**

The **Device and Media Controls** standard requires an organization to implement policies and procedures that control the receipt and removal of hardware and electronic media that contain ePHI and includes the following implementation specifications:

Template: Physical → Policies and Procedures for Device and Media Controls
Template: Physical → Hardware and Electronic Media Tracking Form
Template: Physical → Workstation Reassignment Tracking Form

a. **Disposal (R)**

Establish and implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.

b. **Media Re-Use (R)**

Establish and implement policies and procedures for removal of ePHI from electronic media before the media are made available for re-use

c. **Accountability (A)**

Maintain a record of the movements of hardware and electronic media and any person that is responsible for having modified them.

d. **Data Backup and Storage (A)**

Create a retrievable, exact copy of electronic PHI, when needed, before movement of equipment.

© Copyright 2002-2015, HIPAATraining.com

Step 4. Technical Safeguards

INTRODUCTION

The HIPAA Security Rule's requirements are organized into three categories:

Administrative safeguards	policies and procedures designed to show how the entity will comply with the security rule
Physical safeguards	the controlling of physical access to protect against inappropriate access to protected data
Technical safeguards	the controlling of access to computer systems and the protection of communications containing PHI transmitted electronically over open networks

The third of the HIPAA Security categories, Technical safeguards, is the focus of this step.

Technical safeguards are the technology and the policy and procedures for its use that protect ePHI and control access to it.

The Technical Safeguards consist of the following 5 standards:

- Access Control
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security

NOTE: For employer group health plans, substitute group health plan name for all <organization name> placeholders in documents.

ACTION ITEMS

☐ **1. Access Control**

The **Access Control** standard requires an organization to implement technical policies and procedures that allow only authorized persons or software programs to access ePHI and includes the following implementation specifications:

Template: Technical → Policies and Procedures for Access Control

a. **Unique User Identification (R)**

Assign a unique name and or number for identifying and tracking user identity.

b. **Emergency Access Procedure (R)**

Establish and implement policies and procedures for obtaining necessary ePHI during an emergency

c. **Automatic Logoff (A)**

Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

© Copyright 2002-2015, HIPAATraining.com

d. **Encryption and Decryption (A)**

Implement a mechanism to encrypt and decrypt ePHI

☐ **2. Audit Controls (R)**

The **Audit Controls (R)** standard requires an organization to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

Template: Technical → Policies and Procedures for Audit Controls

☐ **3. Integrity**

The **Integrity** standard requires organizations to implement security measures to ensure that ePHI is not improperly modified without detection until disposed of and includes the following single implementation specification:

Template: Technical → Policies and Procedures for Data Integrity

a. **Mechanism to Authenticate Electronic Protected Health Information (A)**

Establish and implement policies, procedures, and mechanisms to protect ePHI from improper alteration or destruction.

☐ **4. Person or Entity Authentication (R)**

The **Person or Entity Authentication (R)** standard requires an organization to implement policies and procedures to verify that a person or entity seeking access to electronic PHI is the one claimed.

Template: Technical → Policies and Procedures for Person and Entity Authentication

☐ **5. Transmission Security**

The **Transmission Security** standard requires an organization to implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network and includes the following implementation specification:

Template: Technical → Policies and Procedures for Transmission Security

a. **Integrity Controls (A)**

Implement security measures to ensure that electronically transmitted ePHI cannot be easily intercepted and interpreted by anyone other than the intended recipient.

b. **Encryption (A)**

Implement a mechanism to encrypt ePHI whenever deemed appropriate.

© Copyright 2002-2015, HIPAATraining.com

Step 5. Going Forward

INTRODUCTION

If you've reached this final step, then congratulations. You're now to the point where you can declare yourself compliant with the HIPAA Security Regulations.

ACTION ITEMS

☐ **1. Ensure that you have completed all of the steps in this HIPAA to do list.**

Make sure that you have successfully completed each of the previous steps in this checklist.

☐ **2. Pat yourself on the back for a job well done.**

You have completed HIPAATraining.com's HIPAA Security Documentation Kit Program.

☐ **3. Going Forward.**

Make sure and place all your HIPAA Security compliance forms and documents into a binder and store it in a safe place. Remember that HIPAA compliance is not a one-time implementation. Rather, it is an ongoing process and to be effective, must be integrated into your organization's daily processes.

☐ **4. Additional Resources.**

As part of the ARRA/HITECH Act, a regional office privacy advisor in each regional office of the HHS (Department of Health and Human Services) was created and is tasked with offering guidance and education to covered entities, business associates, and individuals on their rights and responsibilities related to Federal privacy and security requirements for PHI. Contact the HHS and obtain the name and contact information for the regional office privacy advisor designated for your region as they can be a great resource for HIPAA related information. For more information, contact the Department of Health and Human Services at 1-877-696-6775 or the Office of Civil Rights ((866)–OCR-PRIV) or (866)627-7748).

Congratulations!!!

© Copyright 2002-2015, HIPAATraining.com