Calendar Year

2012

Enter Facility Name Here

HIPAA Security Compliance Workbook

For Core Measure 15 of Meaningful Use Requirements - Annual Risk Analysis

Administrators Guide

Multi-User Systems

HIPPA Compliance Security Workbook

Statement of Disclaimer

The information contained herein is for the sole purpose of information and education. The information or processes promulgated in this workbook or their usage in your facility is NOT warranted or guaranteed in any fashion. All information published online or in print by DocuTrac, Inc. is subject to change without notice. DocuTrac, Inc. is not responsible for errors or damages of any kind resulting from access or use of the information contained therein. Every effort has been made to ensure the accuracy of information presented as factual; however, errors may exist. Users are directed to countercheck facts when considering their use in their facilities, practices or businesses. DocuTrac, Inc. is not responsible for the content, functionality or usage of the ideas, reports, or logs contained herein, that responsibility rests solely with your facilities, practices or businesses.

Questions or comments on any information listed in this workbook can be addressed by contacting the person listed with the email address at the bottom of this page.

James B. Miller
Director of Quality Assurance and Compliance
DocuTrac, Inc.
20140 Scholar Drive Ste. 218
Hagerstown, MD 21742
800-850-8510 x115
jmiller@quicdoc.com

Table of Contents

INTRODUCTION

This HIPAA Security Compliance Workbook has been prepared to support the (Enter Facility Name) HIPAA Security Initiative. For this phase of the Initiative, each system must be brought into compliance with the HIPAA security regulations. The workbook has been created to assist users in implementing, upgrading and documenting their computing practices in order to achieve HIPAA Security Compliance.

PURPOSE

The workbook is intended to be a "lowest common denominator" guide for users to achieve and maintain satisfactory compliance with the HIPAA security regulations. The "entry level" solutions and procedures presented are not intended to be adopted in their entirety by all users. The workbook can serve as a useful vehicle for high-level, standardized documentation of the various alternative procedures actually employed; a "check-off sheet" to ensure that all required areas have been considered.

ADDITIONAL HIPAA SECURITY REQUIREMENTS

In addition to this Workbook, there are several other HIPAA requirements that may be dealt with at the institutional level. You may be contacted from time to time to participate in those initiatives. For example, HIPAA regulations require that all individuals who use systems that contain Electronic Protected Health Information receive periodic training on security awareness. The Appointed Committee or Individual is preparing training materials. These will be distributed to you at a later date.

AUDIENCE

The intended audiences for the Workbook are the personnel of (Enter Facility Name Here). Many of the services and solutions that are presented in the Workbook are available primarily or exclusively for use on (Enter Facility Name Here) equipment or by (Enter Facility Name Here) employees and staff.

Workbook Organization

The Workbook is composed of nine major sections; each covers a broad area of security requirements. The intent has been to "roll-up" the security requirements into a small number of unified sections. In the process, no attempt has been made to adhere to the order of requirements within the original regulations. Users who wish to view the detailed HIPAA Security regulations will find online references to them in the Workbook Appendix.

MULTI-USER SYSTEMS: ADDITIONAL REQUIREMENTS

This version of the Workbook is intended primarily to document HIPAA Security compliance for Multi-User systems. That is, systems that support multiple user accounts and are routinely used by several individuals. Since the potential risk of unauthorized disclosure may be greater for such systems, HIPAA regulations require the additional safeguards be implemented. Section 9 of the Workbook presents the additional requirements and Standard compliance procedures.

FORMAT

Most Sections contain four subsections:

1. REQUIREMENT. The relevant HIPAA security requirements that apply to the section are briefly itemized and discussed.
2. STANDARD. This subsection presents at least one "acceptable" solution, meeting the requirements of (Enter Facility Name Here). The primary intent is to provide the average user with at least one simple method of meeting the relevant compliance requirements.
3. EQUIVALENT ALTERNATIVE SOLUTION. Many users will not adopt the Standard Solution, as they have alternative methods already in place. They should document their alternative solution in this subsection.
4. Optional LOG SHEETS. In those cases where routine documentation of monitoring and maintenance activities is required, basic Log Sheets are provided for that purpose. The actual Log sheets can be used to maintain the required documentation, or they can serve as a basic template for developing alternative documentation procedures.

GENERAL INSTRUCTIONS

Even though the System may not need to have all the Workbook sections completed in order to achieve compliance, it is a good idea to do so anyway, since the Workbook can serve as a single, standardized source of documentation for future reference.

Step-By-Step Instructions

1. System administrators should complete Sections 1-9 of the Workbook.
2. If any of the manual Log Sheets that are included in the Workbook will be used to document system maintenance activities, they should be prepared for each system listed in Section 1. The Logs should be distributed to the individuals who will actually be performing the maintenance activities.

If you have questions, please review the following:

- http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html

SECTION 1: Catalog of Systems

List all systems that are covered by this Workbook:
(Use additional copies of this page if necessary)

1. Asset Number assigned by (Enter Facility Name Here):

   _____

   System Identification Number assigned by: (Enter Facility Name Here) (Serial number, Property Number, etc)

   _____

   System Description (Dell PC, IBM server, etc):

   _____

   System Location:

   _____

2. Asset Number assigned by (Enter Facility Name Here):

   _____

   System Identification Number assigned by: (Enter Facility Name Here) (serial Property Number, etc)

   _____

   System Description (Dell PC, IBM Server, etc):

   _____

   System Location:

   _____

3. Asset Number assigned by (Enter Facility Name Here):

   _____

   System Identification Number assigned by: (Enter Facility Name Here) (serial Property Number, etc)

   _____

System Description (Dell PC, IBM Server, etc):

System Location:

Responsible Party

These Catalog of Systems Worksheets have been completed by
(Enter Name/Title/Date)

SECTION 2: Physical Security Management

Requirements

1. Systems should be located in physically secure locations, whenever possible. A secure location would minimally be defined as one that is not routinely accessible to the public, particularly if authorized personnel are not always available to monitor security.
2. Secure locations must have physical access controls (Card Key, door locks, etc.) that prevent unauthorized entry, particularly during periods outside of normal work hours, or when authorized personnel are not present to monitor security.
3. Access control systems must be maintained in good working order and records of maintenance, modification and repair activities should be available.
4. Wherever technically feasible, access logs that track incoming and outgoing activities should be reviewed on a periodic basis.
5. Systems located in public areas require special consideration. Every effort should be made to limit the amount of ePHI that is stored on such systems. Auto logoff, screen savers, proximity badge, and other device-specific hardware/software measures should be employed to maximally enhance security.
6. Maintenance records for physical security devices are maintained and available from (Enter Facility Name Here) Plant Operations and Maintenance Division and the Information Services Division.

STANDARD: Physical Security for the System

Physical Access Control measures are in place:

Building Name or Physical Address:

Building Level (Door Locks, Card Key, Controlled elevator access, etc):

Room Level (Door Locks, Card Key, etc):

Device Level (if any additional):

Physical Security Device maintenance records that are available:

SECTION 3: Backup Procedures and Media Destruction

Requirements

1. Backup copies of ePHI must be created and updated on a regular basis.
2. Frequency of backing up is dependent upon how frequently the information is modified, as well as the criticality of the data.
3. Backups may be performed to portable media (examples: CD-ROM, diskette, digital tape, etc.).
4. Alternatively, backup copies may be transferred to network file servers, if the data stored on the servers are backed up on a regular schedule and the archival media is stored in a safe, secure environment. For example, network file servers maintained by (Responsible Party Name Here) are completely acceptable for backup retention.
5. In the event of damage or malfunction of the system, backup media or alternative server data stores must be accessible within a reasonable period of time, in order to provide timely access to the ePHI for patient care or other immediate needs.
6. When portable media is discarded, it should either be overwritten or destroyed, eliminating all possibility that any ePHI contents could be read.
7. When a System is recycled, transferred to another user, or discarded, all storage devices or all ePHI records must be overwritten at least three times, rendering all ePHI records unreadable.
8. Backup Documentation: Backup maintenance should be documented.
9. Backup Log Review: For multi-user systems, the backup logs should be periodically reviewed by the appropriate supervisor or manager.

STANDARD: Backup Procedures

The following backup procedures will be maintained on the system.
Backups will be performed on:

Option 1: Network Server

Server Name:
Server Location:
Drive and Directory Location of Copies:

Option 2: Portable Media

Media Type (CD-ROM, diskette, etc):
Media will be stored at the following location:

Backup Frequency:
Backups will be performed at least every:
Backup Documentation: Backup Maintenance will be documented by using:

1. The included Workbook Backup Log Sheets (see Appendix 2- page 21 for System Backup Log Sheets)
2. Equivalent Alternative:

STANDARD: Manager/Supervisor Review

1. System administrators will use the included Multi-User System Backup Log Sheet that provides entries where supervisors can document their periodic review: (see Appendix 2-page 21)
2. Equivalent Alternative:

STANDARD: Media Destruction

All portable media (diskettes, CD-ROM's, etc) will either be physically rendered unreadable, or all ePHI records will be overwritten at least three times prior to discard or reuse (YES/NO):

STANDARD: System Recycling, Reuse or Discard

All storage devices on the system will either be:
1. Physically rendered unreadable AND/OR
2. Overwritten at least three times.
   (Yes/No):

SECTION 4: Account Management and Access Review

Requirements

1. Each User must be provided a unique account, with a unique User Name and Password.
2. Generic or shared accounts are not permitted.
3. Any written records of Account names and passwords should be kept in a locked, secure environment (not attached to a CRT for easy reference).
4. Access to a User's account must never be shared with another individual.
5. System administrators as well as individual users should maintain the recommended minimum practices for account and password maintenance. In the case where legacy systems cannot technically meet the minimum standards, passwords should reflect the maximum supportable length and complexity.
6. Passwords should be complex. Best practice is that they are composed of multiple character types, including: upper and lowercase alpha characters, numeric characters and symbols (#, $, etc).
7. They should be at least 8 characters in length.
8. Authorization: For multi-user systems that are maintained by system administrators, there should be a formal system for authorizing user access. This may take the form of an account request requiring management approval, or some electronic means of verifying that an account request is legitimate and authorized by the requesting department.
9. Account authorization as well as account management activities should be logged.
10. Management should review Account Logs on a periodic basis.

STANDARD: Account Maintenance Logging

1. The included Multi-User System Account Maintenance Log will be used to document system account activities (see Appendix 2- page 24)
   (Yes/No):

   Equivalent Alternative:

STANDARD: The following password standards will be maintained on the system

Requirement	Standard
Minimum Length	
Upper and Lower Case Supported	
Symbols Supported	
Frequency of Password Change	

STANDARD: Generic Accounts not permitted

Any generic accounts have been removed (Yes/No):

System Access Review

System Administrators should periodically review the appropriate System Access Logs to ensure that there has not been attempted or actual unauthorized access to the system.

Requirements

1. Administrators should familiarize themselves with the various system logs that record successful and unsuccessful login and logoff activity.
2. Logs should be reviewed on a periodic basis. A reasonable standard would be to review logs every two weeks.
3. Documentation of the periodic reviews should be maintained.
4. If suspicious activity is detected, contact (Enter Manager or Supervisor Name Here) for further assistance and guidance.

STANDARD: The following log file review standards will be maintained on the system

1. The System Log File(s) will be reviewed every ____ days.
2. The Access Review Log Sheet will be used to document the reviewed System Log File(s). (see Appendix 2- page 23 for the System Access Review Log Sheet)
   (Yes/No):
   Equivalent Alternative:

SECTION 5: Emergency Access

Requirements

1. Users must ensure that in the event of emergency situations, the ePHI information on the System can be accessed when they are unavailable to provide access through normal means.
2. The procedure for emergency access should be reliable. For example, a system that relies upon the primary user to respond to pager or cell phone messages is not reliable, since there are a variety of likely scenarios wherein the primary user may not receive the message, or respond to it in a timely fashion.
3. The emergency access protocol should be written and should be communicated in advance to multiple individuals within the organization.
4. An acceptable protocol would be to:
    a. Create an account and password with all necessary access privileges
    b. Place the information in a sealed, signed envelope
    c. Place the envelope in a locked, secure location
    d. Notify several responsible individuals within the immediate organization and provide them with the necessary means to access the envelope

STANDARD:

The following emergency access protocol has been established that provides for emergency access to the system during the absence of the primary user.

QuicDoc Enterprise 6.2 allows for the creation of an emergency access code to be assigned to specified personnel. This emergency access code allows full access to all areas of the system. A log record is written of every emergency access and what was performed during that emergency session.

The following individuals who are regularly available in the immediate work area have been informed and are prepared to execute the emergency access protocol.

1.
2.
3.
4.

Section 6: Disaster Recovery Procedures

Requirements

All systems that contain ePHI are susceptible to catastrophic damage or destruction by unforeseen environmental or other causes. Provisions must be made to ensure that ePHI records that are stored on the system are not irretrievably lost, should catastrophic damage or failures occur.

1. ePHI should be archived ("backed up") to portable media on a regular basis. Portable media can include: diskettes, network drives, CD-ROM, digital tape, approved network storage or offsite storage service. See Section 3, "Backup Procedures" for further information on archival requirements.
2. Current copies of the archival media should be stored at a remote location that is unlikely to be affected by a local disaster. This media would be used to retrieve the ePHI, in the event that the system or local archival media are destroyed.
3. A "Disaster Recovery Plan" must be prepared that specifies the procedures to be implemented in order to resume access to ePHI following a disaster.
4. An acceptable Disaster Recovery Plan may consist of one or more of the following (or an equivalent plan developed by the system owner).

Acceptable Disaster Recovery Plans

1. (Enter Facility Name Here) has a comprehensive Disaster Recovery Plan. All ePHI on the system is archived on a regular basis onto a network server that is maintained by (Responsible Party Name Here). In the event of a disaster, (Responsible Party Name Here) will provide for recovery of the ePHI.
2. Data is archived on a regular basis onto portable media and stored at a Remote Location. The format of the archival media is compatible with systems that are maintained in the (Enter Facility Name or Location Here) and for which comprehensive disaster recovery facilities are available. In the event of a disaster, remotely stored copies of the media will be retrieved by (Responsible Party Name Here) and the comprehensive Disaster Recovery Plan will assist in the recovery of the ePHI records.
3. Copies of media are remotely stored as in option 2. A system located remotely is to be made available that will be used to recover the ePHI.

STANDARD: The following Disaster Recovery Plan will be implemented in the event of catastrophic loss of the primary system.

Option 1

1. ePHI will be archived to a network file server that is maintained by (Responsible Party Name Here).
2. The name of the server and the directory location of the data are as follows:
3. ePHI data will be archived to the network server every (day, week, etc.)
4. In the event of a disaster, (Responsible Party Name Here) will be contacted, who will arrange for recovery and access to the ePHI.

Option 2

1. ePHI will be archived to portable media on a regular basis; at least once every .
2. Archival media type and format are as follows (example: CD-ROM, Windows 2000 format):
3. Archival media will be labeled as follows:
4. Copies of the archival media will be stored at the following remote location (give specific location information):

Option 3

1. In the event of catastrophic loss of the primary system, an alternative system will be used to recover the ePHI. The alternate system(s) is located at:

   Equivalent Alternative Plan:

Disaster Plan Notification

The following individuals have been informed of this Disaster Recovery Plan and are prepared to execute it (Name, Title, Contact Information).

1.
2.
3.
4.

SECTION 7: Email- Appropriate Use Requirements

Requirements

1. The (Enter Facility Name Here) Email Policy specifies that any email communications that contain ePHI must use an email system approved by (Enter Facility Name Here). No restrictions apply to any email messages that do not contain ePHI.
2. For email communications internal to the (Enter Facility Name Here), both sender and receiver must use the (Enter Facility Name Here) Email System.
3. Email communications to outside email systems that contain ePHI are strongly discouraged unless the message is encrypted.

STANDARD: Email Security Procedures

Email is sent/received on the system (yes/no):

If email is sent/received on the system, usage adheres to (Enter Facility Name Here) Requirements 7.1 listed above (yes/no):

The following email encryption methodology will be used:

SECTION 8: System Security Management Practices

Requirement

1. Systems should be kept current with software upgrades (patches) that correct security deficiencies or enhance the capability to prevent unauthorized access.
2. Software patches are generally provided to licensed customers free of charge by software vendors. Users should subscribe to all available software upgrade services and install new security patches as they become available. Information regarding the availability of security and other software patches for Microsoft software may be found at the Microsoft Corporation Website: Microsoft.com.
3. Systems should have Virus Protection Software installed.
4. The Virus (or Worm) Protection Software should be regularly updated by downloading the latest virus information files; in order to protect the System from infection by newly identified viruses.

STANDARD: System Patches

Systems will be regularly upgraded with current security patches by using the following update procedures:

1. Patches will be obtained from the software vendor and installed on a regular basis.

STANDARD: Virus Protection Software

One or more of the following procedures will be used to keep current with the latest Virus Information Files available for the Virus Protection Software:

1. I will regularly download Virus Information Files from the Application Vendor:
2. Equivalent Alternative:

STANDARD: Auto Logoff

1. The Systems have been configured to Auto-Logoff after the following period of inactivity:
2. Alternative: The system has been configured for a password-protected screensaver after the following period of inactivity:
3. QuicDoc Enterprise 6.2 allows for the Administrator to preset the logoff time under the User Preferences screen. Administrator set auto logoff period ____minutes.

Appendix 1: Contact Information and HIPAA Regulations References

HIPAA Regulations References:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html

HHS Web Site:
http://aspe.hhs.gov/admnsimp/index.shtml

For more information:

- Office for Civil Rights – Privacy of Health Records- (http://www.hhs.gov/ocr/privacy/)
- Am I a covered entity?- (http://www.cms.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp)
  A decision tool developed by DHHS

Appendix 2: Log Sheets for Multi-User Systems

1. Backup Log Sheet
2. System Access Review Log
3. System Account Maintenance Log

MULTIUSER SYSTEM BACKUP LOG SHEET

Use this Log Sheet to document regular backup procedures. Separate Log Sheets should be maintained for each System covered by this Workbook.

System Identification

Description:

Serial or Property Number:

Location:

Activity Log

Date	Operator	Incremental Back-up Date	Full Back-up Date	Offsite Copy Update

Manager/Supervisor Review and Comments

Date	Manager Identification	Comments

System Access Review Log

Use this log sheet to document the periodic review of Computer Access Logs

System Identification

Description:

Serial or Property Number:

Location:

Date	Reviewer	Findings

Multi-User System Account Maintenance Log

Use this log sheet to document the following Account activities:

- Authorization
- Creation
- Deletion
- Inactivation
- Password change

System Identification

Description:

Serial or Property Number:

Location:

Date	Person	Authorization	Account Name	Function (Create/Delete/ Password Change)	Performed By

For multi-user systems maintained by a system administrator, the supervisor or manager should periodically review the Account Management logs

Manager/Supervisor Review and Comments

Date	Manager Identification	Comments

Appendix 3: What to do in case of a Security Breach

In case of a privacy or security breach, how *should* your organization react?

In the healthcare setting, patient information is extremely sensitive, with records containing social security numbers and detailed medical history. As such, an organization must have an action plan in place and always be ready to defend its infrastructure as well as respond appropriately — and in a timely fashion – to any breaches of data.

When a breach occurs in healthcare, meaning that there was an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information, such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual, then the following steps must be taken:

Local authorities notification and report filing:

- Notify the local police and file a police report with the details
- Internal organization notification:

Notify the IT director, CIO, security officer, legal team, appropriate administrators, etc.

- Begin taking steps based on any existing procedures to isolate or take offline the affected systems in order to stop further unauthorized access

Contact security groups:

- Enlist assistance from security experts to ensure that all unauthorized access is blocked
- Perform system analysis to ensure no other systems have been compromised

Notify any authorities and entities listed under the breach notification from DHHS:

- In August of 2009, HHS issued final breach notification regulations which required HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. HHS required the following steps after a breach of unsecured protected Health information (as listed in the HHS web site)

- ***Individual Notice***

Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site or by providing

the notice in major print or broadcast media where the affected individuals likely reside. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity. Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their protected health information was involved in the breach.

- ***Media Notice***

Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

- ***Notice to the Secretary***

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

- ***Notification by a Business Associate***

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no

later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any information required to be provided by the covered entity in its notification to affected individuals.