NIST Special Publication 800-66

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

# An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

**Pauline Bowen, Arnold Johnson, Joan Hash**
**Carla Dancy Smith, Daniel I. Steinberg**

I N F O R M A T I O N  S E C U R I T Y

**DRAFT**

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

***May 2004***


**U.S. Department of Commerce**
*Donald L. Evans, Secretary*

**Technology Administration**
*Phillip J. Bond, Under Secretary of Commerce for Technology*

**National Institute of Standards and Technology**
*Arden L. Bement, Jr., Director*

## Reports on Information Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology promotes the United States economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof-of-concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of non-national- security-related information in federal information systems. This Special Publication 800 series reports on ITL's research, guidelines, and outreach efforts in information system security and its collaborative activities with industry, government, and academic organizations.

## Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, that provide adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

## Acknowledgments

The authors wish to thank their colleagues who reviewed working drafts of this document and contributed to its development.

The Centers for Medicare and Medicaid Services' involvement with the National Institute of Standards and Technology (NIST) and NIST workgroups does not, and shall not be deemed to, constitute the endorsement, recommendation, or approval of any NIST product or publication, by the Department of Health and Human Services, the Centers for Medicare and Medicaid Services, or the Office of HIPAA Standards.

# TABLE OF CONTENTS

**TABLE OF CONTENTS** ..... **iv**

**Executive Summary** ..... **vi**

**1. Introduction** ..... **1**

1.1 Purpose and Applicability ..... 2
1.2 Scope ..... 3
1.3 Organization of This Special Publication ..... 3

**2. NIST IT Security Publications** ..... **5**

2.1 Security Program Development Life Cycle ..... 6
2.2 Publications Directly Supporting Federal Requirements for System Certification and Accreditation (C&A) ..... 7

**3. HIPAA Security Rule** ..... **11**

3.1 HIPAA Goals and Objectives ..... 11
3.2 Security Rule Organization ..... 11
3.3 Safeguards Included in the HIPAA Security Rule ..... 12

**4. Associating NIST Publications with HIPAA Security Requirements Standards** ..... **15**

**Administrative Safeguards** ..... **16**

4.1 Security Management Process (§164.308(a)(1)) ..... 16
4.2 Assigned Security Responsibility (§164.308(a)(2)) ..... 19
4.3 Workforce Security (§164.308(a)(3)) ..... 21
4.4 Information Access Management (§164.308(a)(4)) ..... 23
4.5 Security Awareness and Training (§164.308(a)(5)) ..... 25
4.6 Security Incident Procedures (§164.308(a)(6)) ..... 28
4.7 Contingency Plan (§164.308(a)(7)) ..... 30
4.8 Evaluation (§164.308(a)(8)) ..... 33
4.9 Business Associate Contracts and Other Arrangements (§164.308(b)(1)) ..... 36

**Physical Safeguards** ..... **38**

4.10 Facility Access Controls (§164.310(A)(1)) ..... 38
4.11 Workstation Use (§164.310(b)) ..... 41
4.12 Workstation Security (§164.310(c)) ..... 43
4.13 Device and Media Controls (§164.310(d)(1)) ..... 44

**Technical Safeguards** ..... **46**

4.14 Access Controls (§164.312(a)(1)) ..... 46
4.15 Audit Controls (§164.312(b)) ..... 48
4.16 Integrity (§164.312(c)(1)) ..... 50
4.17 Person or Entity Authentication (§164.312(d)) ..... 52
4.18 Transmission Security (§164.312(e)(1)) ..... 54

**Appendix A— References** ..... **55**

**Appendix B— Glossary** ..... **57**

**Appendix C— Acronyms** ..... **63**

**Appendix D— HIPAA Security Rule/NIST Publications Crosswalk** ..... **64**

**Appendix E— HIPAA Security Rule/FISMA Requirements Crosswalk .....71**

## Executive Summary

Some Federal agencies, in addition to being subject to the Federal Information Security Management Act of 2002 (FISMA), are also subject to (in many areas) similar requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule (the Security Rule).

This Special Publication (SP) summarizes the HIPAA security standards and explains some of the structure and organization of the Security Rule. This SP helps educate readers about security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security safeguards set out in the Rule. This publication is also designed to direct readers to helpful information in other National Institute of Standards and Technology (NIST) publications on individual topics the HIPAA Security Rule addresses. Readers can draw upon these publications for consideration in implementing the Security Rule. This publication is intended as an aid to understanding security concepts discussed in the HIPAA Security Rule, does not supplement, replace, or supersede the HIPAA Security Rule itself.

The HIPAA Security Rule specifically focuses on the safeguarding of electronic protected health information (EPHI). Although FISMA applies to all federal agencies and all information types, only a subset of agencies is subject to the HIPAA Security Rule based on its use of EPHI. All covered entities under HIPAA must comply with the HIPAA Security Rule, which establishes a set of security standards for protecting certain health care information. In general, the standards, and implementation specifications of HIPAA apply to the following covered entities, including federal agencies and their contractors and service providers that meet the following descriptions:

- **Health Care Providers—**Any provider of medical or other health services, or supplies, that transmits any health information in electronic form in connection with a transaction for which a standard has been adopted.
- **Health Plans—**Any individual or group plan that provides or pays the cost of health care.
- **Health Care Clearinghouses—**A public or private entity that processes health care transactions from a standard format to a nonstandard format, or vice-versa.

NIST standards and guidelines can be used to support the requirements of both HIPAA and FISMA.

Title III of the E-Government Act of 2002 (Public Law 107-347), which recognized the importance of information security to the economic and national security interests of the United States, tasked NIST with responsibilities for creating security standards and guidelines, including the development of the following:

- Standards to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels
- Guidelines recommending the types of information and information systems to be included in each category
- Minimum information security requirements (i.e., management, operational, and technical controls), for information and information systems in each such category.

FISMA directs heads of federal agencies and their chief information officers (CIOs) to ensure that there is an information security program in place and trained personnel assigned to manage and support the program. Heavy emphasis is placed on fully integrating security in the business processes. Preparation of

security plans and certification and accreditation of agency systems are critical to meeting the objectives of FISMA. In many areas both FISMA and the HIPAA Security Rule specify similar requirements.

NIST security publications (Special Publications in the 800 series and Federal Information Processing Standards (FIPS)) may be used by organizations to provide a structured, yet flexible framework for selecting, specifying, employing, and evaluating the security controls in information systems. For federal organizations, the information provided by these publications can make a significant contribution toward satisfying the requirements of FISMA and HIPAA.

.

## 1. Introduction

Among its responsibilities, the National Institute of Standards and Technology (NIST) is responsible for developing standards and guidelines, including minimum requirements, used by federal agencies in providing adequate information security for the protection of agency operations and assets. Pursuant to this mission, NIST's Information Technology Laboratory (ITL) has developed guidance to improve the efficiency of information technology (IT) planning, implementation, management, and operation.

NIST publishes a wide variety of guidance publications on information security. These publications serve as a valuable resource for federal agencies seeking to address existing and new Federal information security requirements. One such set of federal information security requirements is the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Public Law104-191). HIPAA required the Secretary of the Department of Health and Human Services (HHS) to adopt security standards for certain kinds of health information. These standards, known as the HIPAA Security Rule (the Security Rule), were published on February 20, 2003. In the preamble to the Security Rule, several NIST guidance publications were cited as potentially valuable resources to readers with specific questions and concerns about IT security.

This Special Publication helps educate readers about security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security safeguards set out in the Security Rule. It is designed to point readers to helpful information in other NIST publications on individual topics the HIPAA Security Rule addresses. Readers can draw upon these publications for consideration in implementing the Security Rule. Use of the referenced NIST publications is not required for compliance with the Security Rule.

Congress enacted HIPAA to simplify and standardize health care administrative processes, thereby reducing costs and other burdens on the health care industry. The HIPAA statute is comprised of five Titles, some of which address health care industry concerns such as health care insurance coverage and health care finance. Title II, however, includes the HIPAA administrative simplification requirements that address how electronic health care transactions are transmitted and stored. Pursuant to these provisions of HIPAA, the Secretary of HHS adopted several sets of rules (in addition to the Security Rule) to implement the HIPAA administrative simplification requirements.

HHS has published proposed or final rules related to the following five components of health care industry practices:

- Code sets used to identify health care services
- Identifiers used for unique designations for employers and health care providers
- Electronic data interchange transactions
- Security
- Privacy.

This document addresses only the security component of the HIPAA statute.

Figure 1 shows all the components of HIPAA and illustrates that the focus of this document is on the security provision of the statute and the regulatory rule.

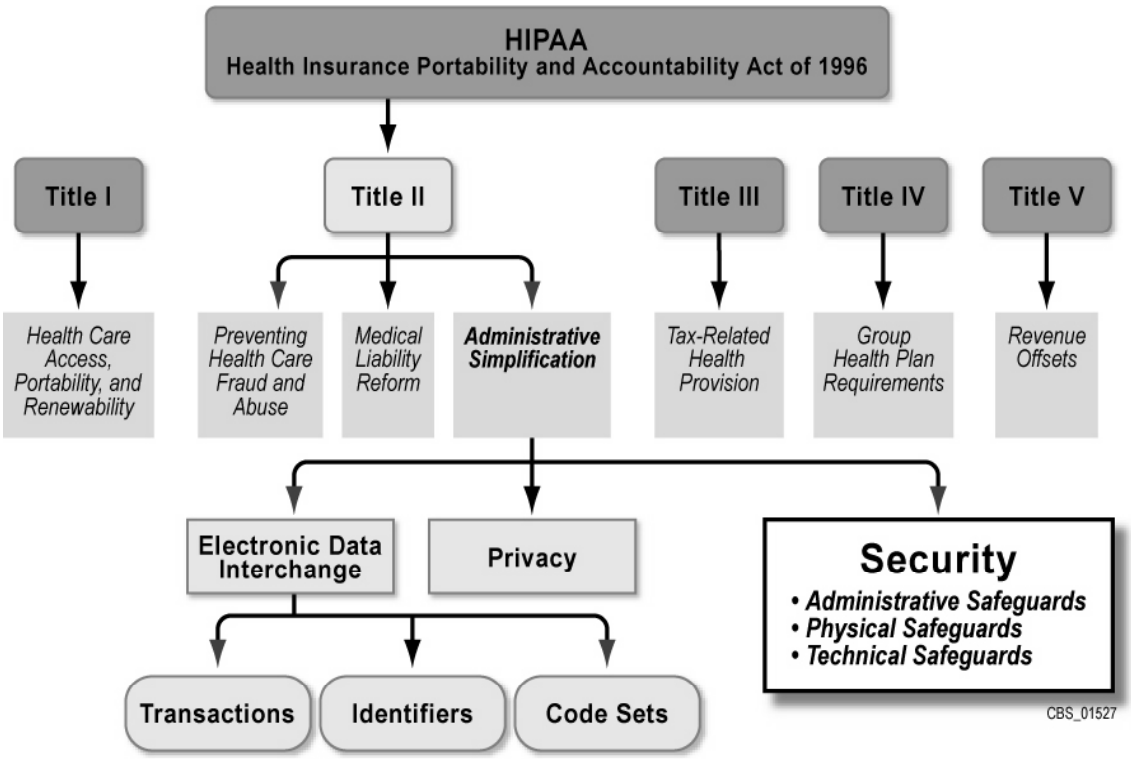


**Figure 1. HIPAA Components**

"Covered entities" (except small health plans) must comply with the Final Security Rule by April 21, 2005, and small health plans must comply by April 21, 2006.[1] Readers may refer to the Centers for Medicare and Medicaid Services (CMS) web site, http://www.cms.hhs.gov/hipaa/hipaa2, for more detailed information about the passage of the HIPAA law by Congress, specific provisions of HIPAA, determination of the entities covered under the law, the complete text of the HIPAA Security Rule, the deadline for compliance with the Rule, and enforcement information.

## 1.1 Purpose and Applicability

The purpose of this Special Publication (SP) is to help educate readers about IT security concepts included in the HIPAA Security Rule. This document is also designed to direct readers to helpful information in other NIST publications on individual topics addressed by the HIPAA Security Rule. Readers can draw upon these publications for consideration in implementing the Security Rule.

The guidance provided in this SP is applicable to all federal information systems,[2] other than those systems designated as national security systems as defined in 44 United States Code (U.S.C.), Section 3542.[3] The guidance included in this publication has been broadly developed from a technical perspective

[1] In defining a "small health plan," the Security Rule indicates that it adopts the same definition as the rule codifying another HIPAA Administrative Simplification provision, the Transactions Rule: A "small" health plan is one with annual receipts of $5 million or less.

[2] A Federal information system is an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

[3] A national security system is any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation of use of which: involves intelligence activities, involves cryptographic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct

so as to be complementary to similar guidelines issued by agencies and offices operating or exercising control over national security systems. State, local, and tribal governments, as well as private sector organizations comprising the critical infrastructure of the United States are encouraged to consider using these guidelines, as appropriate.

NIST publications may be useful to any organization seeking to understand the security issues raised by the HIPAA Security Rule regardless of that organization's size, structure, or distribution of security responsibilities. Specific agency missions, resources, and organizational structures, however, vary greatly, and staff members who will have roles and responsibilities for implementing the HIPAA Security Rule may vary widely from organization to organization. Federal agencies use different titles to identify roles that have security-related responsibilities and may also allocate particular responsibilities for implementing information security controls (those required by HIPAA and others) differently. NIST SP 800-66 assists all agencies seeking further information on the security safeguards discussed in the HIPAA Security Rule, regardless of the particular structures, methodologies, and approaches used to address its requirements.

## 1.2 Scope

This publication provides a brief overview to the HIPAA Security Rule and directs the reader to additional NIST publications on IT security. It addresses those topics within the HIPAA Security Rule that are most common to readers seeking information.

This publication is intended as an aid to understanding security concepts discussed in the HIPAA Security Rule, and does not supplement, replace, or supersede the Security Rule itself. Anyone seeking clarifications of the HIPAA Security Rule should contact the Office of HIPAA Standards at CMS. Readers may send questions to askhipaa@cms.hhs.gov or contact the CMS HIPAA Hotline, 1-866-282-0659. This hotline was established for the specific purpose of providing assistance with questions related to HIPAA and its requirements.

The NIST publications available as of the publication date of SP 800-66 were used in preparing this document. NIST frequently publishes new standards and guidelines or updates existing publications that may also serve as useful references. To remain current with the latest available list of NIST security publications, the reader should periodically review the NIST Computer Security Resource Center (CSRC) web site at http://csrc.nist.gov.

## 1.3 Organization of This Special Publication

This publication is composed of the following four sections and five appendices.

**Section 1** gives an overview of the purpose and scope of the document and identifies the intended audience.

**Section 2** provides an overview of this Special Publication and its relationship to other NIST publications and specific regulations concerning information security.

---

fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. Agencies should consult NIST Special Publication 800-59, *Guide for Identifying an Information System as a National Security System*, for guidance on determining the status of their information systems.

**Section 3** explains some of the key concepts included in the HIPAA Security Rule.

**Section 4** maps supporting NIST standards and guidance to the HIPAA security standards contained in the HIPAA Security Rule.

**Appendix A** lists related references and source material.

**Appendix B** defines terms used in this document.

**Appendix C** identifies and defines acronyms used within this document.

**Appendix D** provides a crosswalk of the HIPAA Security Rule to available NIST publications that readers may draw upon for consideration in implementing the Security Rule.

**Appendix E** provides a crosswalk of the requirements of the HIPAA Security Rule to the requirements of the Federal Information Security Management Act of 2002 (FISMA), which contains requirements relevant to the security programs of all federal agencies.

## 2. NIST IT Security Publications

Special Publication 800-66 was developed by the CSD of NIST's ITL pursuant to its mission regarding the development of guidance for IT security planning, implementation, management, and operation. Guidance prepared by the CSD includes publications that address many security areas that are impacted by the HIPAA Security Rule. These publications may be valuable to readers with specific questions and concerns. Table 1 lists the NIST publications identified in NIST SP 800-66. To identify which of these publications can be used to support the implementation of each of the security safeguards of the HIPAA Security Rule, see the *HIPAA Security Rule / NIST Publications Crosswalk* in Appendix D. The publications referred to in Table 1 and in Appendix D are available for download from NIST's web site at http://csrc.nist.gov/publications/.

**Table 1. NIST Publications Referenced in NIST SP 800-66**[4]

| NIST Publication | Title |
|---|---|
| FIPS 140-2 | *Security Requirements for Cryptographic Modules* |
| FIPS 199 | *Standards for Security Categorization of Federal Information and Information Systems* |
| NIST SP 800-12 | *An Introduction to Computer Security: The NIST Handbook* |
| NIST SP 800-14 | *Generally Accepted Principles and Practices for Securing Information Technology Systems* |
| NIST SP 800-16 | *Information Technology Security Training Requirements: A Role- And Performance-Based Model* |
| NIST SP 800-18 | *Guide for Developing Security Plans for Information Technology Systems* |
| NIST SP 800-26 | *Security Self-Assessment Guide for Information Technology Systems* |
| NIST SP 800-27 | *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)* |
| NIST SP 800-30 | *Risk Management Guide for Information Technology Systems* |
| NIST SP 800-34 | *Contingency Planning Guide for Information Technology Systems*. |
| NIST SP 800-35 | *Guide to Information Technology Security Services* |
| NIST SP 800-36 | *Guide to Selecting Information Security Products* |
| NIST SP 800-37 | *Guide for the Security Certification and Accreditation of Federal Information Systems* |
| NIST SP 800-42 | *Guideline on Network Security Testing* |
| NIST SP 800-44 | *Guidelines on Securing Public Web Servers* |
| NIST SP 800-47 | *Security Guide for Interconnecting Information Technology Systems* |
| NIST SP 800-50 | *Building Information Technology Security Awareness and Training Program* |
| NIST SP 800-53 | *Recommended Security Controls for Federal Information Systems* |
| NIST SP 800-55 | *Security Metrics Guide for Information Technology Systems* |
| NIST SP 800-56 | *Recommendation on Key Establishment Schemes* |
| NIST SP 800-57 | *Recommendation on Key Management* |
| NIST SP 800-59 | *Guideline for Identifying an Information System as a National Security System* |
| NIST SP 800-60 | *Guide for Mapping Types of Information and Information Systems to Security Categories* |
| NIST SP 800-61 | *Computer Security Incident Handling Guide* |
| NIST SP 800-63 | *Recommendation for Electronic Authentication* |
| NIST SP 800-64 | *Security Considerations in the Information System Development Life Cycle* |

## 2.1 Security Program Development Life Cycle

The HIPAA Security Rule safeguards address various phases of the security program life cycle. The life cycle phases include planning of security controls and policies, implementation of security controls, assessment of the security of an IT system or program, and technical and IT infrastructure guidance. An

[4] Status and most current versions of the NIST documents (Draft or Final) can be found at http://csrc.nist.gov/publications.

organization seeking to address issues in a particular phase of the security program life cycle may wish to focus its attention on NIST publications most relevant to that program phase. Figure 2 identifies NIST publications that may be most helpful to an organization seeking more information on security-related issues in the development stages shown below.

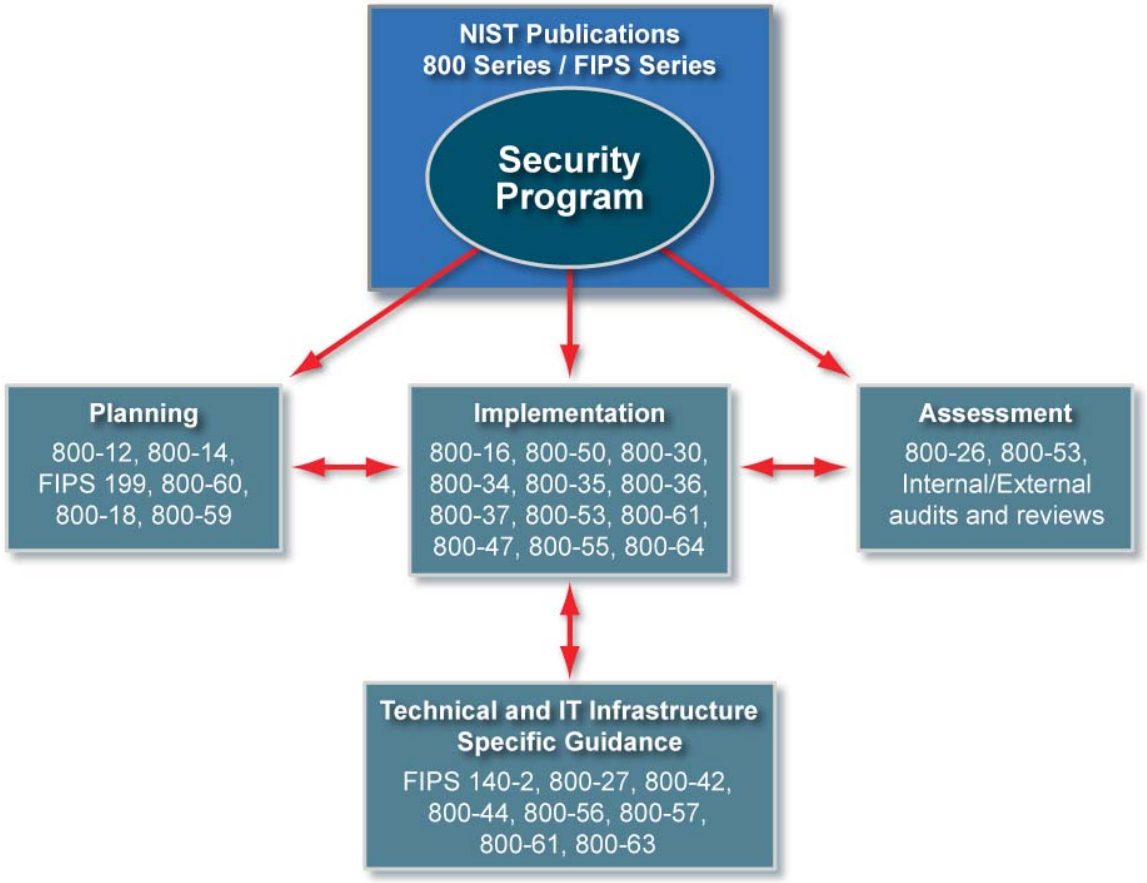


**Figure 2. Key Publications for Establishing and Supporting a Security Program**

## 2.2 Publications Directly Supporting Federal Requirements for System Certification and Accreditation (C&A)

The E-Government Act of 2002 (Public Law 107-347) recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (FISMA), tasked NIST with responsibilities for standards and guidelines, including the development of the following:

- Standards to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels
- Guidelines recommending the types of information and information systems to be included in each category

- Minimum information security requirements (i.e., management, operational, and technical controls) for information and information systems in each such category.

FISMA directs heads of federal agencies and their Chief Information Officers (CIOs) to ensure that there is an information security program in place and trained personnel assigned to manage and support the program. Heavy emphasis is placed on fully integrating security into the business processes. One of the most critical processes important to ensuring that proper security controls are included in agency systems is the process, which provides an assessment of whether the security controls have been implemented and are operating as intended. Coupled with this activity is the requirement that a management official authorize each system for operation. These processes are known as certification and accreditation (C&A). ***FISMA requires that agency systems be certified and accredited***. This includes federal systems subject to HIPAA. Figure 3 below highlights key publications essential to achieving system certification and accreditation regarding security controls and the sequence in which they should be considered.

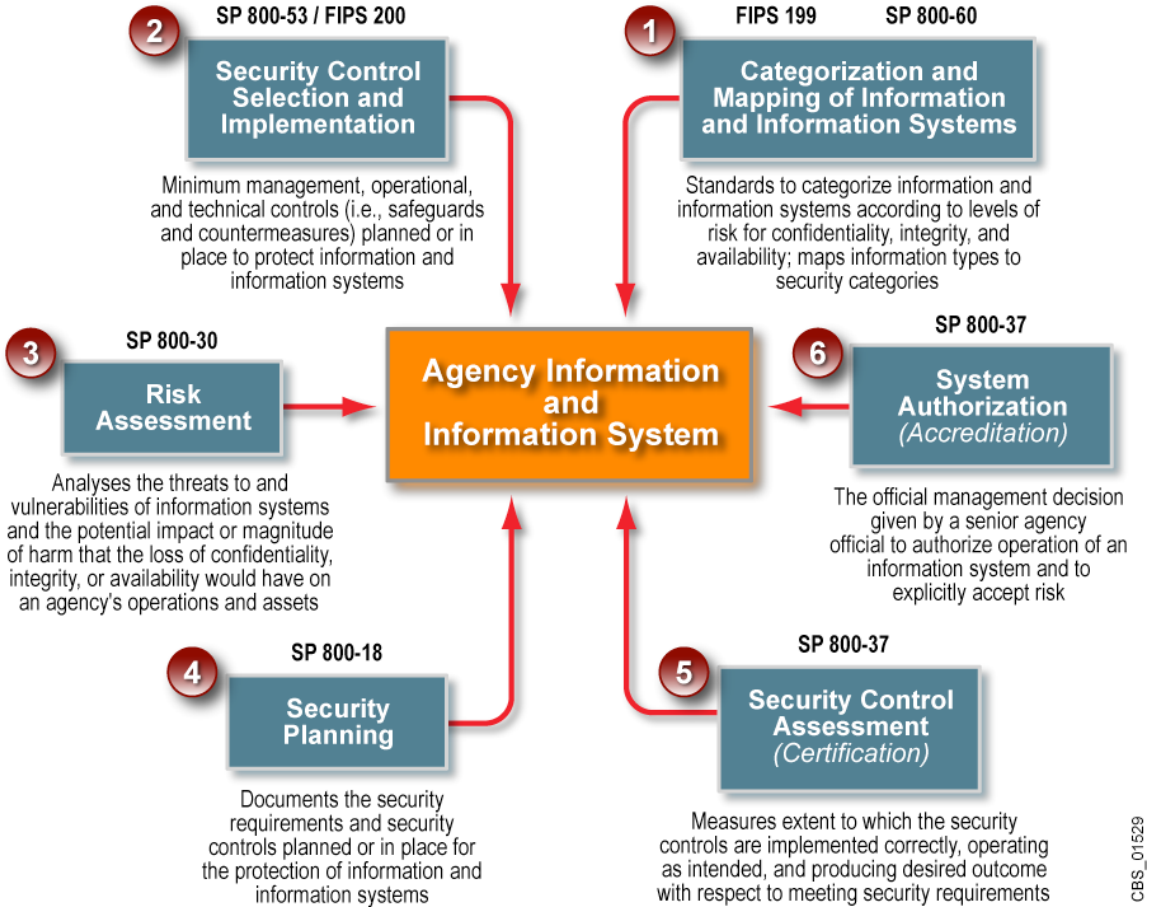


**Figure 3. NIST Publications Directly Supporting Federal C&A Requirements**

Following is a brief overview of the topics covered in each of the NIST publications identified in Figure 3. Included with each overview is a brief description of how the document supports other publications in Figure 3.

***Federal Information Processing Standards (FIPS) 199 Overview***

- Presents standards for categorizing information and information systems based on the objective of providing appropriate levels of information security according to a range of risk levels.
- Illustrates the security level used as an indicator (called "security category") of how severely an agency mission can be potentially impacted (i.e., Low, Moderate, or High) if the worst-case scenario occurs from loss of confidentiality, integrity, and/or availability of information.
- Aligns security categories to recommended initial baseline sets of security controls from SP 800-53 to be used as the starting point for risk analysis activities.

***SP 800-60 Overview***

- Identifies various/typical information types found in federal agencies and discusses these in the context of the FIPS 199 security categories.
- Provides a recommended methodology for mapping information types to a security category.
- Discusses and applies the methodology to specific information types as examples of how to use the methodology.
- When possible, identifies information types that should have the same security category across all federal agencies.

***SP 800-53/FIPS 200 Overview*** [5]

- Provides a catalog of security controls for information systems (derived from many sources).
- Recommends baseline security controls for information systems (in accordance with FIPS 199 security categories).
- Provides guidance for agency-directed tailoring of baseline security controls based on risk/cost-benefit analyses.
- Defines security control baselines (minimum) for Low, Moderate, and High for security categories in accordance with FIPS 199.

***SP 800-30 Overview***

- Provides guidance on risk management techniques and methods.
- Focuses on assessment of magnitude of harm based on issues related to confidentiality, integrity, and availability.

***SP 800-18 Overview***

- Provides guidance on preparation of system security plans.
- Identifies key security components for both application and general support systems.

[5] NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, provides interim guidance until completion and adoption as FIPS 200.

***SP 800-37 Overview***

- Establishes guidelines (including tasks and subtasks) to certify and accredit information systems supporting the executive branch of the federal government.
- Applies to information systems, which are not national security systems as defined in FISMA.

# 3. HIPAA Security Rule

The HIPAA Security Rule specifically focuses on the safeguarding of electronic protected health information (EPHI). Although FISMA applies to all federal agencies and all information types, only a subset of agencies is subject to the HIPAA Security Rule based on its use of EPHI. All covered entities under HIPAA must comply with the HIPAA Security Rule, which establishes a set of security standards for securing certain health care information. In general, the standards of HIPAA apply to the following covered entities including federal agencies that meet the following descriptions:

- **Health Care Providers—**Any provider of medical or other health services, or supplies, that transmits any health information in electronic form in connection with a transaction for which a standard has been adopted.
- **Health Plans—**Any individual or group plan that provides or pays the cost of health care.
- **Health Care Clearinghouses—**A public or private entity that processes health care transactions from a standard format to a nonstandard format, or vice-versa.

This section summarizes the HIPAA security standards and explains some of the structure and organization of the Security Rule.

## 3.1 HIPAA Goals and Objectives

The main goal of the HIPAA Security Rule is to protect the confidentiality, integrity, and availability of electronic protected health information.

- **Confidentiality** is "the property that data or information is not made available or disclosed to unauthorized persons or processes."
- **Integrity** is "the property that data or information has not been altered or destroyed in an unauthorized manner."
- **Availability** is "the property that data or information is accessible and usable upon demand by an authorized person."

## 3.2 Security Rule Organization

To understand the requirements of the HIPAA Security Rule, it is helpful to be familiar with the basic security terminology it uses to describe the security measures. By understanding the requirements and the terminology in the HIPAA Security Rule, it becomes easier to see which NIST publications may be appropriate reference resources and where to find more information. Each security measure of the HIPAA Security Rule can be categorized as being an Administrative, Physical, or Technical safeguard.

- **Administrative Safeguards** are defined as the "administrative actions, policies, and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."
- **Physical Safeguards** are defined as the "security measures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion."

- **Technical Safeguards** are defined as the "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."

Each security safeguard can also be categorized as being either a standard or an implementation specification. An "implementation specification" is a more detailed description of the method or approach covered entities can use to meet a particular standard. ***Each set of safeguards is composed of a number of specific implementation specifications that are either required or addressable***. If an implementation specification is described as required, the specification must be implemented. If it is addressable, then the covered entity must assess whether each implementation specification is a reasonable and appropriate safeguard in its environment. If the covered entity chooses not to implement a specification, the entity must either document the reason or implement an alternative measure. Anyone seeking clarification regarding the principles of the HIPAA Security Rule should send inquiries to the CMS e-mail box, askhipaa@cms.hhs.gov, or contact the CMS HIPAA Hotline, 1-866-282-0659.

### 3.3 Safeguards Included in the HIPAA Security Rule

Table 2 lists the safeguards of the HIPAA Security Rule. This table provides a quick reference of the standards and implementation specifications of the Security Rule categorized by administrative, physical, or technical safeguards. Column 1 of the table lists the HIPAA standard, column 2 indicates the relevant section of the Security Rule where the standard can be found, and column 3 lists the implementation specification.

These categories of safeguards encompass the continuum of security for electronic health care information for covered entities under HIPAA. The security process begins with the policies and procedures that establish personnel behavior and provides a framework for acceptable access to and uses of protected health information. These administrative controls are the foundation for the HIPAA Security Rule. The physical safeguards support limitations to restricted spaces and equipment, including materials that contain electronic protected health information. The final category of safeguards delineated in the HIPAA Security Rule is the group of technical safeguards. These controls apply specifically to information systems and are measures of protection associated with the actual hardware, software, and networks for these systems.

***NOTE***: ***In many areas both FISMA and the HIPAA Security Rule specify similar requirements. Appendix E of this document provides a comparison between the two.***

**Table 2. HIPAA Security Standards and Implementation Specifications[6]**

| Standards | Sections | Implementation Specifications (R)=Required (A)=Addressable | |
|---|---|---|---|
| **Administrative Safeguards** | | | |
| Security Management Process | 164.308(a)(1) | Risk Analysis (R)<br>Risk Management (R) | Sanction Policy (R)<br>Information System Activity Review (R) |
| Assigned Security Responsibility | 164.308(a)(2) | [None] | |
| Workforce Security | 164.308(a)(3) | Authorization and/or Supervision (A)<br>Workforce Clearance Procedure (A)<br>Termination Procedures (A) | |
| Information Access Management | 164.308(A)(4) | Isolating Health Care Clearinghouse Function (R)<br>Access Authorization (A)<br>Access Establishment and Modification (A) | |
| Security Awareness and Training | 164.308(a)(5) | Security Reminders (A)<br>Protection from Malicious Software (A)<br>Log-in Monitoring (A)<br>Password Management (A) | |
| Security Incident Procedures | 164.308(a)(6) | Response and Reporting (R) | |
| Contingency Plan | 164.308(a)(7) | Data Backup Plan (R)<br>Disaster Recovery Plan (R)<br>Emergency Mode Operation Plan (R)<br>Testing and Revision Procedure (A)<br>Applications and Data Criticality Analysis A) | |
| Evaluation | 164.308(a)(8) | [None] | |
| Business Associate Contracts and Other Arrangements | 164.308(b)(1) | Written Contract or Other Arrangement (R) | |
| **Physical Safeguards** | | | |
| Facility Access Controls | 164.310(a)(1) | Contingency Operations (A)<br>Facility Security Plan (A)<br>Access Control and Validation Procedures (A)<br>Maintenance Records (A) | |
| Workstation Use | 164.310(b) | [None] | |
| Workstation Security | 164.310(c) | [None] | |
| Device and Media Controls | 164.310(D)(1) | Disposal (R)<br>Media Re-use (R) | Accountability (A)<br>Data Backup and Storage (A) |
| **Technical Safeguards** | | | |
| Access Control | 164.312(a)(1) | Unique User Identification (R)<br>Emergency Access Procedure (R) | Automatic Logoff (A)<br>Encryption and Decryption (A) |
| Audit Controls | 164.312(b) | [None] | |
| Integrity | 164.312(c)(1) | Mechanism to Authenticate Electronic Protected Health Information (A) | |
| Person or Entity Authentication | 164.312(d) | [None] | |
| Transmission Security | 164.312(e)(1) | Integrity Controls (A) | Encryption (A) |

[6] Adapted from 68 Federal Register 8380, February 20, 2003 (Appendix A to Subpart C of Part 164--Security Standards: Matrix).

Pursuant to its mission under FISMA, NIST has prepared publications that are relevant to the standards and implementation specifications listed in Table 2. In the following section, security measures relevant to these safeguards from NIST publications are presented, along with references to publications that may be useful in considering how to approach implementing the HIPAA Security Rule standards.

## 4. Associating NIST Publications with HIPAA Security Requirements Standards

This section associates the NIST publications with the respective Security Rule topic standards to facilitate their use in applying the HIPAA Security Rule. Each HIPAA Security Rule standard is outlined in a tabular module format. The modules provide an overview of the information available in NIST's IT Security publications. The modules are composed of the following components:

The ***Key Activities*** column lists for each HIPAA Security Rule standard some suggested key activities that are usually associated with a particular security function. The activities are not all-inclusive, and there will be many additional activities an organization will need to consider, specific to its own operations. Note that the HIPAA Security Rule itself associates several "implementation specifications" for each standard, as listed in Table 2 and Appendices D and E. Not all modules address all of the standard's associated implementation specifications, as they are meant to serve as a general introduction to the security topics raised by the standards of the HIPAA Security Rule. For more detailed information about the key activities, consult one or more NIST publications referenced for the subject HIPAA standard.

The ***Description*** column in the table/module includes an expanded explanation about the key activities. The descriptions include types of activities an organization may pursue in addressing a specific security function. These are abbreviated explanations designed to help get an organization started in addressing the HIPAA Security Rule. The NIST publications identified for this HIPAA standard can be consulted for more detailed information about the security topic.

The third column, ***Sample Questions***, includes representative questions to determine whether or not the elements described have actually been considered or completed. These sample questions are not exhaustive but merely representative. They are a starting point for an organization to examine its security practices as they relate to the HIPAA Security Rule. Affirmative answers to these questions do not imply that an organization is meeting all of the requirements of the HIPAA security requirement. If an organization has already incorporated considerations raised by these questions into its information security program, however, those efforts may signal that the organization is taking appropriate steps. In fact, it is expected that many organizations with existing information security infrastructure already in place will have considered the Sample Questions. Questions should be tailored to fit the unique circumstances of each entity.

The ***Examples*** at the end of the HIPAA standard module are meant to illustrate how the standard may be addressed in a specific environment based on a set of objectives. They are only representative, not all-inclusive. The actual activities necessary to implement the standard requirement for any given entity may vary substantially depending on organization mission, size, and scope. The examples are for illustrative purposes only and are not meant to imply any degree of HIPAA compliance. In many cases, the examples are also written to reflect possible approaches for small and resource-constrained environments.

For each HIPAA security standard noted in the following section, there are one or more NIST publications identified that readers will find helpful and relevant to each standard. ***Introductory references*** provide basic concepts relevant to the standard. ***Primary references*** reflect more detailed treatment of the specific standard and ***supplemental references*** can be used to provide additional information beyond the introductory and primary references. These may be appropriately applied based on the individual organization's mission, size, and scope. These publications are also referenced in the HIPAA Security Rule/ NIST Publications Crosswalk table in Appendix D.

## Administrative Safeguards

### 4.1 Security Management Process (§164.308(a)(1))

**HIPAA Standard**: *Implement policies and procedures to prevent, detect, contain, and correct security violations.*

| Key Activities | Description | Sample Questions |
|---|---|---|
| | **Introductory Reference***: An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12 - Chapter 5)* | |
| **1. Identify Relevant Information Systems** | • Identify all information systems that house individually identifiable health information.<br>• Include all hardware and software that are used to collect, store, process, or transmit protected health information.<br>• Analyze business functions and verify ownership and control of information system elements as necessary. | • Has all hardware and software for which the organization is responsible been identified?<br>• Is the current information system configuration documented, including connections to other systems?<br>• Have the types of information and uses of that information been identified and the sensitivity of each type of information been evaluated? (See FIPS 199 and SP 800-60 for more on categorization of sensitivity levels.) |
| **2. Conduct Risk Assessment** | Risk assessments typically include the following steps:<br>• Determine system characterization:<br>– Hardware<br>– Software<br>– System interfaces<br>– Data and information<br>– People.<br>• System mission.<br>• Identify any vulnerability or weaknesses in security procedures or safeguards.<br>• Identify events that can negatively impact security.<br>• Identify current controls in place<br>• Identify the potential impact that a security breach could have on an organization's operations or assets, including loss of integrity, availability, or confidentiality.<br>• Recommend security controls for the information and the system, including all the technical and non- technical protections in place to address security concerns.<br>• Determine residual risk.<br>• Document all outputs and outcomes from the risk assessment activities. | • Are there any prior risk assessments, audit comments, security requirements, and/or security test results?<br>• Is there intelligence available from agencies, the Office of the Inspector General (OIG), the Federal Computer Incident Response Center (FedCIRC), mass media, virus alerts, and/or vendors?<br>• What are the current and planned controls?<br>• Is the facility located in a region prone to any natural disasters, such as earthquakes, floods, or fires?<br>• Has responsibility been assigned to check all hardware and software to determine whether selectedl security settings are enabled?<br>• Is there an analysis of current safeguards and their effectiveness relative to the identified risks? |

| Key Activities | Description | Sample Questions |
|---|---|---|
| **3. Acquire IT Systems and Services** | Although the HIPAA Security Rule does not require purchasing any particular technology, additional hardware, software, or services may be needed to adequately protect information. Considerations for their selection should include the following:<br>• Applicability of the IT solution to the intended environment.<br>• The sensitivity of the data<br>• The organization's security policies, procedures, and standards<br>• Other requirements such as resources available for operation, maintenance, and training. | • How well will new security controls work with the existing IT architecture?<br>• Have the security requirements of the organization been compared with the security features of existing or proposed hardware and software?<br>• Has a cost- benefit analysis been conducted to determine the reasonableness of the investment given the security risks identified?<br>• Has a training strategy been developed? |
| **4. Create and Deploy Policies and Procedures** | Document the decisions concerning the management, operational, and technical controls selected to mitigate identified risks<br>• Create policies that clearly establish roles and responsibilities and assign ultimate responsibility for the implementation of each control to particular individuals or offices<br>• Create procedures to be followed to accomplish particular security related tasks. | • Are policies and procedures in place for security?<br>• Are there user manuals available and are they up-to-up to date?<br>• Is there a formal (documented) system security plan?<br>• Is there a formal contingency plan?<br>• Is there a process for communicating policies and procedures to the affected employees?<br>• Are policies and procedures reviewed and updated as needed? |
| **Supplemental NIST References** | • NIST SP 800-14<br>• NIST SP 800-18<br>• NIST SP 800-26<br>• NIST SP 800-27<br>• NIST SP 800-30<br>• NIST SP 800-37<br>• NIST SP 800-53<br>• NIST SP 800-60<br>• FIPS 199 | |

### Example 1:

A small health care service organization has decided to move its manual scheduling system to a web-based application. It has decided to ask its internal security team to conduct a risk assessment prior to implementation to identify necessary controls, which should be included within the design in order to protect the information. After completing its assessment, the team recommends that the organization install a firewall, upgrade its virus detection and containment software, and also implement an automated access control function and an audit capability. In addition, the team emphasizes the need for the organization to develop a user manual and complete user training before implementation.

### Example 2:

A very large health care organization assembles a task force to review current sanction policies related to employees' failure to follow existing procedures related to handling and disclosure of health care information. The review indicates that current personnel policies covering employee misuse and/or abuse of system privileges are broad enough to address the area of health care information. Current sanction penalties range from written reprimands to suspensions and terminations. In special circumstances, procedures exist to initiate criminal prosecution. The company's Human Resources department provides support in interpretation and application of these procedures. The review recommends the addition of an update to the access authorization forms currently being signed by all system users before they receive approval to access the system. It is suggested that specific reference to electronic health care information be added to the form in addition to the categories currently delineated.

## 4.2 Assigned Security Responsibility (§164.308(a)(2))

**HIPAA Standard:** *Identify the security official who is responsible for the development and implementation of the policies and procedures required.*

| Key Activities | Description | Sample Questions |
|---|---|---|
| | **Introductory Reference***: An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12 – Chapter 3)* | |
| **1. Select a Security Official To Be Assigned Responsibility for HIPAA Security** | • Identify the individual who will ultimately be responsible for security.<br>• Select an individual who is able to assess effective security and to serve as the point of contact for Security policy, implementation, and monitoring. | Who in the organization—<br>• Oversees the development and communication of security policies and procedures?<br>• Is responsible for conducting the risk assessment?<br>• Handles the results of periodic security evaluations?<br>• Directs IT security purchasing and investment?<br>• Ensures that security concerns have been addressed in system implementation? |
| **2. Assign and Document the Individual's Responsibility** | • Document the individual's responsibilities in a job description<br>• Communicate this assigned role to the entire organization. | • Is there a complete job description that accurately reflects assigned security duties and responsibilities?<br>• Have the staff members in the organization been notified as to whom to call in the event of a security problem? |
| **Supplemental NIST References** | • NIST SP 800-14<br>• NIST SP 800-26<br>• NIST SP 800-53 | |

### Example 1:

The head of a small (10 employees) health care service provider organization has been reviewing HIPAA standards and realizes that they must formally assign a person to be responsible for HIPAA implementation. Currently no one on staff has the expertise in security needed to do the job. They have two choices: (1) train an existing employee or (2) hire a new resource. From a cost perspective, they would prefer to train existing staff. They have three IT specialists on staff that currently support the small local area network (LAN) installed one year ago. They believe that, it would not be difficult to train a resource from this operation to coordinate HIPAA security implementation. They have also asked the training manager to identify recommended sources so that a comprehensive training strategy can be developed. The new function will also be discussed at the weekly staff meeting..

### Example 2:

A large urban health organization hires a consultant to design its HIPAA security program. The consultant reviews job descriptions and interviews the Chief Technology Officer, the Privacy Officer, the Chief Information Officer, and the Executive Officer. The consultant notes that security responsibilities are currently assigned to an "IT Security Committee," not a specific individual identified by name, title,

or both as required by the HIPAA Security Rule. The consultant recommends that a specific member of the IT Security Committee be designated as the organization's Security Officer responsible for the overall HIPAA Security program, including HIPAA implementation. The Director Implements the recommendations and ensures that the newly defined function is reflected in the clinic's documented security policy under "Roles and Responsibilities".

## 4.3 Workforce Security (§164.308(a)(3))

**HIPAA Standard:** *Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.*

| Key Activities | Description | Sample Questions |
|---|---|---|
| | **Introductory Reference***: An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12 – Chapter 17)* | |
| **1. Establish Clear Job Descriptions and Responsibilities** | • Define roles and responsibilities for all job functions.<br>• Assign appropriate levels of security oversight, training, and access.<br>• Identify in writing who has the business need—and who has been granted permission—to view, alter, retrieve, and store electronic health information, and at what times, under what circumstances, and for what purposes. | • Are there written job descriptions that are correlated with appropriate levels of access?<br>• Is there an implementation strategy that supports the designated access authorities? |
| **2. Establish Criteria and Procedures for Hiring and Assigning Tasks** | • Ensure that staff members have the necessary knowledge, skills, and abilities to fulfill particular roles, e.g., positions involving access to and use of sensitive information.<br>• Ensure that these requirements are included as part of the personnel hiring process. | • Are applicants' employment and educational references checked?<br>• Have appropriate background checks been completed? |
| **3. Establish Termination Procedures** | • Develop a standard set of procedures that should be followed to recover access control devices (Identification [ID] badges, keys, access cards, etc.) when employment ends.<br>• Deactivate computer access accounts (e.g., disable user IDs and passwords). See the Access Controls Standard. | • Are there separate procedures for voluntary termination (retirement, promotion, change of employment) vs. involuntary termination (termination for cause, reduction in force, involuntary transfer, and criminal or disciplinary actions)?<br>• Is there a standard checklist for all action items that should be completed when an employee leaves (return of all access devices, deactivation of logon accounts, delivery of any needed data solely under the employee's control)? |
| **Supplemental NIST References** | • NIST SP 800-14<br>• NIST SP 800-26<br>• NIST SP 800-53 | |

### Example 1:

The IT System Administrator for a small health clinic maintains a log of staff members with system access accounts. The log is a table listing names, job positions, start dates, and termination dates. Job positions are correlated with sensitivity levels and systems access. The sensitivity levels and system access privileges define what specific types of electronic health information an individual can touch, view, retrieve, alter, transmit, and/or store, and under what circumstances, and for what purposes. There is also a field that lists the new hire and annual refresher training completion dates and the dates that system access was granted. This documentation log is periodically reviewed and updated as required based on workforce turnover and changes.

### Example 2:

A large hospital establishes procedures for terminating employees for cause. The supervisor collects access cards and ID badges immediately. Security staff members escort employees while they recover their personal items and exit the facility. Before the termination, the supervisor calls the IT department to shut off any access the subject employee has to the IT system, especially access to sensitive information and individually identifiable health information (including written information). Physical access and IT system audit logs for the previous month are reviewed to determine whether the employee made any unusual or inappropriate attempts to access electronic protected health information. Based on this analysis, a plan of action for corrective action is developed.

### 4.4 Information Access Management (§164.308(a)(4))[7]

**HIPAA Standard:** *Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.*

| Key Activities | Description | Sample Questions |
|---|---|---|
| | **Introductory Reference**: *An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12 – Chapter 17)* | |
| **1. Determine Criteria for Establishing Access** | • Decide how the person with the assigned security responsibility will consistently grant access to others within the organization<br>• Document which process will be used to select the **basis** for restricting access<br>• Choose between identity- based access (by name) or role-based access (by job or by other appropriate means). | • Does the organization's IT operating system have the capacity to set access controls?<br>• Are there documented job descriptions that accurately reflect assigned duties and responsibilities and enforce segregation of duties?<br>• Will access be identity-based, role-based, location-based, or some combination thereof? |
| **2. Determine Who Should Be Authorized to Access Information Systems** | • Establish **standards** for granting access<br>• Provide formal authorization from the appropriate authority before granting access to sensitive information. | • Are duties separated such that only the minimum necessary electronic health information is made available to each staff member based on their job requirements? |
| **3. Evaluate Existing Security Measures Related to Access Controls** | • Evaluate access controls already in place or implement new access controls as appropriate<br>• Coordinate with other existing management, operational, and technical controls, such as policy standards and personnel procedures, maintenance and review of audit trails, identification and authentication of users, and physical access controls. | • Are access policies reviewed and updated routinely?<br>• Do all employees receive appropriate security training?<br>• Are authentication mechanisms used to verify the identity of those accessing systems?<br>• Does management regularly review the list access authorizations and update as necessary?<br>• What policies and procedures are already in place for access control safeguards? |
| **Supplemental NIST References** | • NIST SP 800-14<br>• NIST SP 800-18<br>• NIST SP 800-53<br>• NIST SP 800-63 | |

### Example 1:

A doctor's office uses an operating system with system administration functionalities. All office staff and physicians may need to access patient health or billing records in the course of performing their duties. Among these individuals, it is impractical to restrict access to electronic health information given the size of the office and the multiple functions each person must perform. The office manager assigns a unique identification number and password to all office staff and health care practitioners, allowing them access to all electronic health information. Custodial staff, vendors, and others with whom a business

[7] Note: Supports the Facility Access Controls Physical Standard and the Access Controls Technical Standard.

relationship exists do not receive access authorization and are not allowed to log on to any computer or the LAN.

### Example 2:

A health clinic implements user ID and password controls. It also requires a second password to access applications other than administrative support and appointment scheduling applications, e-mail, and web services. Staff members needing access to billing and patient record applications to perform their duties must be authorized to access these systems after receiving training on these programs. In addition, software used to access sensitive health information is only installed on workstations for employees whose assigned job functions require such access.

## 4.5 Security Awareness and Training (§164.308(a)(5))

**HIPAA Standard:** *Implement security awareness and training program for all members of its workforce (including management).*

| Key Activities | Description | Sample Questions |
|---|---|---|
| | **Introductory Reference**: *An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12 – Chapter 13)* | |
| **1. Conduct a Training Needs Assessment** | • Determine the training needs of the organization.<br>• Interview and involve key personnel in assessing, security training needs. | • What awareness, training, and education programs are needed (e.g., what is required)?<br>• What is the current status regarding how these needs are being addressed (e.g., how well are current efforts working)?<br>• Where are the gaps between the needs and what is being done (e.g., what more needs to be done)?<br>• What are the training priorities? |
| **2. Develop and Approve a Training Strategy and a Plan** | • Address the specific HIPAA policies that require awareness and training in the written training strategy.<br>• Outline in the written training plan the scope of the awareness and training program; the goals; the target audiences; the learning objectives; the deployment methods, evaluation, and measurement techniques; and the frequency of training. | • Is there a procedure in place to ensure that everyone in the organization receives security awareness training?<br>• What type of security training is needed to address specific technical topics based on job responsibility?<br>• When should training be scheduled to ensure that compliance deadlines are met?<br>• Is security awareness discussed with all new hires?<br>• Are security topics reinforced during routine staff meetings? |
| **3. Develop Appropriate Awareness and Training Content; Create Training Materials; and Determine Best Delivery Methods** | Select the topics that may need to be included in the training materials such as the following:<br>– Security reminders<br>– Incident reporting<br>– How to protect and guard the system from malicious software<br>– Procedures for detecting and reporting malicious software<br>– Procedures for monitoring log-in attempts and reporting discrepancies<br>– Password management and use.<br>• Use new and "hot" information from e-mail advisories, online IT security daily news web sites, and periodicals.<br>• Deliver training information to staff in the easiest and most cost-efficient manner.<br>• Consider using a variety of media and avenues according to what is appropriate for the organization based on workforce size, location, level of education, etc. | • Have employees received a copy of or do they have easy access to the security procedures and policies?<br>• Do employees know whom to contact and how to handle a security incident?<br>• Do employees understand the consequences of noncompliance with the stated security policy?<br>• Are employees who travel aware of both physical laptop security issues and information security issues and how to handle them?<br>• Do employees know the importance of timely application of system patches?<br>• Have we researched available training resources?<br>• Is there in-house training staff?<br>• What is the security training budget? |

| | | |
|---|---|---|
| **4. Implement the Training** | • Schedule and conduct the training outlined in the strategy and plan<br>• Implement any reasonable technique to disseminate the security messages in an organization, including newsletters, screensavers, videotapes, e-mail messages, teleconferencing sessions, staff meetings, and computer-based training. | • Have all employees received adequate training to fulfill their security responsibilities?<br>• What methods are available or already in use to make employees aware of security, e.g., posters or booklets? |
| **5. Monitor and Evaluate Training Plan** | • Keep the security awareness and training program fresh and current.<br>• Conduct training whenever changes occur in the technology and practices as appropriate.<br>• Monitor the training program implementation to ensure all employees participate.<br>• Implement corrective actions when problems arise. | • Are employee training and professional development programs documented and monitored?<br>• Is there annual security refresher training?<br>• How are new employees trained on security? |
| **Primary Reference**<br><br>**Supplemental NIST References** | • NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*<br><br>• NIST SP 800-14<br>• NIST SP 800-16<br>• NIST SP 800-53 | |

### Example 1:

A large hospital has security staff members who recently completed an information systems awareness and training needs assessment. The security staff is now developing an awareness and training plan to help them meet those needs. It has been determined that all staff members who have access to patient information must attend an information security awareness briefing annually. This requirement is extended to any contractors, either in-house or working external to the hospital facilities. The requirement also applies to any other person who has access to hospital-maintained patient information and other information that management deems to be worth protecting from improper disclosure, manipulation, or denial of availability.

The awareness briefing will include specific guidance on protecting sensitive information. The awareness and training plan will identify how that awareness briefing will be presented. The awareness briefing will probably be made available on videotape or on the hospital's LAN. The briefing will also be presented in classroom presentations for those staff that prefer that approach. Regardless of how the awareness message is made available, the security staff will maintain a database of those who need to receive the awareness briefing and will track who has attended the briefing.

The awareness briefings will be reinforced continually with posters, distribution of information security trinkets, security messages and slogans available for computer screensavers, and occasional facility-wide e-mail messages and advisories.

The awareness and training plan will also document the need for specific groups of staff to receive specialized security training because of their role in the hospital. The information security staff members already know that they will need additional training to meet the technical and managerial challenges they are facing. They also know that the IT support staff (e.g., system administrators, web site administrators,

communication specialists, PC/laptop support staff, and help desk staff) need functional training to enhance their ability to protect the systems that process and store the hospital's data.

The awareness and training plan will be routed for review and approval among the various hospital administrators—some of whom are the IT system owners and data owners. The administrators will have responsibility for helping the security staff implement the plan. The security staff may develop awareness material specifically for hospital management, before proceeding with the awareness and training plan.

### Example 2:

A small family practice doctor's office must certify annually that proper licenses for practicing medicine and operating a business are current. As part of this annual review of operations, the doctor's practice is incorporating a status report on its information security efforts, including a section that is an awareness and training plan.

One person – the office manager – has been designated as the office's information security manager. They advise the three physicians, two physicians' assistants, three nurses, and seven office staff members that they will all need to receive a security awareness briefing – a PC-based tool that the office manager has procured. Several information security posters will be hung in high-traffic areas, and a list of security "do and don't" items will be routed to all staff.

The doctor's office will contact the local businesses that provide its IT support (e.g., PC, Internet, office communications) and accounts receivable/payable services. The office will suggest meetings be held to discuss how these businesses protect any office/patient information they may have a need to access, and how they train their own employees in information security, including any information security certifications they may require their support staff to acquire and maintain.

## 4.6 Security Incident Procedures (§164.308(a)(6))

**HIPAA Standard**: *Implement policies and procedures to address security incidents.*

| Key Activities | Description | Sample Questions |
|---|---|---|
| | **Introductory Reference:** *An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12 – Chapter 12)* | |
| **1. Determine Goals of Incident Response** | • Gain an understanding as to what constitutes a true security incident—something identified as a security breach or an attempted "hack"—in the organization's environment.<br>• Determine how the organization will respond to a security breach.<br>• Establish a reporting mechanism and a process to coordinate responses to the security incident.<br>• Provide direct technical assistance, advise vendors to address product-related problems, and provide liaisons to legal and criminal investigative groups as needed. | • Has the HIPAA-required security risk assessment resulted in a list of potential physical or technological events that could result in a breach of security?<br>• Is there a procedure in place for reporting and handling incidents?<br>• Has an analysis been conducted that relates each potential security incident to possible results?<br>• Have the key functions of the organization been prioritized to determine what would need to be restored first in the event of a disruption? |
| **2. Develop and Deploy an Incident Response Team** | • Identify appropriate individuals to be a part of a formal incident response team, when required. | • Do members of the team have adequate knowledge of the organization's hardware and software?<br>• Do members of the team have the authority to speak for the organization to the media, law enforcement, and clients or business partners?<br>• Has the incident response team received appropriate training in incident response activities? |
| **3. Develop Incident Response Procedures** | • Document incident response procedures that can provide a single point of reference to guide the day-to-day operations of the incident response team.<br>• Review incident response procedures, solicit input, and make changes to reflect input.<br>• Update the procedures as required based on changing organizational needs. | • Does the organization's size and mission suggest that a staffed security incident hotline be maintained?<br>• Does the organization need standard incident report templates to ensure that all necessary information related to the incident is documented and investigated?<br>• Has the organization determined under what conditions information related to a security breach will be disclosed to the media?<br>• Have appropriate (internal and external) persons who should be informed of a security breach been identified and a contact information list prepared?<br>• Has a written incident response plan been developed and provided to the team? |

| | | |
|---|---|---|
| **4. Incorporate Post-Incident Analysis into Updates and Revisions** | • Measure effectiveness and update security incident response procedures to reflect lessons learned, and make recommendations for improvements to security controls after a security incident. | • Does the incident response team keep adequate documentation of security incidents that list what weaknesses were exploited and how access to information was gained?<br>• Do records reflect new contacts and resources identified for responding to an incident?<br>• Does the organization consider whether current procedures were adequate for responding to a particular security incident? |
| **Primary Reference**<br><br>**Supplemental NIST References** | • NIST SP 800-61,*Computer Security Incident Handling Guide*<br><br>• NIST SP 800-14<br>• NIST SP 800-53 | |

### Example 1:

In the event of a significant security incident, all staff members at a government agency are instructed to contact their Incident Response Team, which includes the Security Officer as a member. The Incident Response Team will evaluate the incident and ensure that it is reported to appropriate management personnel and the FedCIRC. The team members will also inform their investigative organization in the Inspector General's Office if the incident may potentially involve system abuse or criminal activity.

### Example 2:

A small doctor's office is burglarized. After working with emergency services to verify that the physical safety of individuals has not been compromised, the doctor requests assistance from the IT staff and internal audit unit to determine whether any protected health information has been compromised. The doctor reviews what data can be restored from off-site backup servers and takes corrective action, including the purchase and installation of a new intrusion detection system.

## 4.7 Contingency Plan (§164.308(a)(7))

**HIPAA Standard:** *Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.*

| Key Activities | Description | Sample Questions |
|---|---|---|
| | **Introductory Reference:** *An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12 – Chapter 11)* | |
| **1. Develop Contingency Planning Policy** | • Define the organization's overall contingency objectives<br>• Establish the organizational framework, roles, and responsibilities for this area<br>• Address scope, resource requirements, training, testing, plan maintenance, and backup requirements. | • What are the primary missions of the organization?<br>• What services must be provided within specified critical timeframes?<br>• Patient treatment, for example, may need to be performed without disruption<br>• By contrast, claims processing may be delayed during an emergency with no long-term damage to the organization<br>• Have cross-functional dependencies been identified so as to determine how the failure in one system may negatively impact another one? |
| **2. Conduct an Impact Analysis *(Applications and Data Criticality Analysis)*** | • Identify the activities and material that are critical to business operations<br>• Identify the critical services or operations and the manual and automated processes that support them<br>• Determine the amount of time the organization can tolerate power outages, disruption of services, and/or loss of capability<br>• Establish cost-effective strategies for recovering these critical services or processes. | • What hardware, software, and personnel are critical to daily operations?<br>• What is the impact on desired service levels if these critical assets are not available?<br>• What, if any, support is provided by external providers (Internet service providers [ISPs], utilities, or contractors)?<br>• What is the nature and degree of impact on the operation if any of the critical resources are not available? |
| **3. Identify Preventive Measures** | • Identify preventive measures for each defined scenario that could result in loss of a critical service operation<br>• Ensure identified preventive measures are practical and feasible in terms of their applicability in a given environment. | • What alternatives for continuing operations of the organization are available in case of loss of any critical function/resource?<br>• What is the cost associated with the preventive measures that may be considered?<br>• Are the preventive measures feasible (affordable and practical for the environment)?<br>• What plans, procedures, or agreements need to be initiated to enable implementation of the preventive measures, if they are necessary? |

| | | |
|---|---|---|
| **4. Develop Recovery Strategy** | • Finalize the set of contingency procedures that should be invoked for all identified impacts, including emergency mode operation. The strategy must be adaptable to the existing operating environment and address allowable outage times and associated priorities identified in step 2<br>• Ensure, if part of the strategy depends on external organizations for support, that formal agreements are in place with specific requirements stated. | • Have agreed-upon procedures for each possible type of impact identified been documented?<br>• Has a coordinator who manages, maintains, and updates the plan been designated?<br>• Has an emergency call list been distributed to all employees? Have recovery procedures been documented?<br>• Has a determination been made regarding when the plan needs to be activated (anticipated duration of outage, tolerances for outage or loss of capability, impact on service delivery, etc.)? |
| **5. Develop the Contingency Plan** | • Document all the decisions made in the previous steps. | • Is there a written plan?<br>• Does it address both disaster recovery and data backup? |
| **6. Plan Testing, Training, and Execution** | • Test the contingency plan on a predefined cycle (stated in the policy developed under step 1)<br>• Train those with defined plan responsibilities on their roles<br>• If possible, involve external entities (vendors, alternative site/service providers) in testing exercises<br>• Make key decisions regarding how the testing is to occur ("tabletop" exercise versus staging a real operational scenario including actual loss of capability)<br>• Decide how to segment the type of testing based on the assessment of business impact and acceptability of sustained loss of service. Consider cost. | • How is the plan to be tested?<br>• Does testing lend itself to a phased approach?<br>• Is it feasible to actually take down functions/services for the purposes of testing?<br>• Can testing be done during normal business hours or must it take place during off hours?<br>• If full testing is infeasible, has a "tabletop" scenario (classroom-like exercise) been considered?<br>• How frequently is the plan to be tested (annually)?<br>• When should the plan be revised? |
| **Primary Reference**<br><br>**Supplemental NIST References** | • NIST SP 800-34,*Contingency Planning Guide for Information Technology Systems*<br><br>• NIST SP 800-14<br>• NIST SP 800-18<br>• NIST SP 800-26<br>• NIST SP 800-30<br>• NIST SP 800-53 | |

### Example 1:

A small doctor's office (five people) is receiving calls for appointments. As the scheduler is taking patient information to set up an appointment, the office computer system goes down. The caller is anxious to see the doctor as soon as possible due to recurring pain and is concerned about completing the transaction. The scheduler knows that on average, the computer is seldom down for more than an hour, so she invokes the contingency procedure used for minimum outage. The scheduler gives the patient the next available appointment and writes the information down in a log and will transfer the appointment information to the computer system once power is restored. This procedure has been chosen as the most cost- effective

for the office based on established service-level thresholds. (Callers should be able to establish an appointment on the same day the call is initially made.)

### Example 2:

A small health care organization rents an office located on the first floor of an office building in a high crime area of a major metropolitan city. Potential for theft of its computer equipment is a real concern. In response to this concern, the office has established contingency procedures to address loss of critical electronic information due to theft. Copies of important electronic files are made weekly and stored in a lockable, fireproof file cabinet located onsite. The health care organization is also negotiating for new rental space on an upper floor and will pay fees to support a roaming guard service that protects the building after hours. The organization has also negotiated with an outside vendor currently supporting the office's operations to use the vendor's headquarters site (located 30 miles away) as a backup site for storing the information monthly.

## 4.8 Evaluation (§164.308(a)(8))

**HIPAA Standard:** *Perform a periodic technical and non technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.*

| Key Activities | Description | Sample Questions |
|---|---|---|
| | **Introductory Reference***: An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12 – Chapter 9)* | |
| **1. Determine Whether Internal or External Evaluation Is Most Appropriate** | • Decide whether the evaluation will be conducted with internal staff resources or external consultants<br>• Engage external expertise to assist the internal evaluation team where additional skills and expertise is required<br>• Use internal resources to supplement an external source of help, because these internal resources can provide the best institutional knowledge and history of internal policies and practices. | • Which staff has the technical experience and expertise to evaluate the systems?<br>• How much training will staff need on security-related technical and non technical issues?<br>• What are the credentials required for an outside vendor?<br>• What is the budget for internal resources to assist with an evaluation?<br>• What is the budget for external services to assist with an evaluation?<br>• Can other external organizations provide assistance if needed? |
| **2. Develop Standards and Measurements for All Areas and Topics of Security** | • Use an evaluation strategy and tool that has substance and can be tracked, such as a questionnaire or checklist, because documentation is key to demonstrating compliance.<br>• Implement tools that can provide reports on the level of compliance, integration, or maturity of a particular security safeguard.<br>• If available, engage corporate, legal, or regulatory compliance staff when conducting the analysis.<br>• Leverage any existing reports or documentation that may already be prepared by the organization addressing compliance, integration, or maturity of a particular security safeguard. | • Have management, operational, and technical issues been considered?<br>• Do the elements of the evaluation procedure (questions, statements, or other components) address individual, measurable security safeguards?<br>• Has the procedure been developed and tested in a few areas or systems?<br>• Is the procedure supportive of objectives contained in FISMA and HIPAA?<br>• Does the evaluation tool consider all standards and implementation specifications of the HIPAA Security Rule? |
| **3. Conduct Evaluation** | • Determine, in advance, what departments and/or staff will participate in the evaluation.<br>• Secure management support for the evaluation process to ensure participation.<br>• Collect and document all needed information.<br>Collection methods may include the following:<br>– Interviews | • Have staff members with knowledge of IT security been consulted and included in the evaluation team?<br>• Has specifically worded, written approval from senior management been received for any penetration testing?<br>• Has the process been formally communicated to those who have been assigned roles and |

| | | |
|---|---|---|
| | – Surveys<br>– Outputs of automated tools, such as access control auditing tools, system logs, and results of penetration testing.<br>• Penetration testing is a security testing method where trusted insiders attempt to compromise system security for the sole purpose of testing the effectiveness of security controls. | responsibilities in the evaluation process?<br>• Is an automated tool available to support the evaluation process? |
| **4. Document Results** | • Analyze the evaluation results.<br>• Identify security weaknesses.<br>• Document in writing every finding and decision.<br>• Develop security program priorities and establish targets for continuous improvement. | • Does the process support development of security recommendations?<br>• Has a report been written that highlights key findings and recommendations?<br>• Have steps been taken to ensure that the final report is made available only to those persons designated to receive it? |
| **5. Repeat Evaluations Periodically** | • Establish the frequency of evaluations, taking into account the sensitivity of the EPHI controlled by the organization, its size and complexity, and other relevant laws or accreditation requirements.<br>• Repeat evaluations when significant changes to the security environment are made; for example, if new technology is adopted or if there are newly recognized risks to the security of the information. | • Do security policies specify that evaluations will be repeated when changes are made to security practices or the IT system?<br>• Do policies on frequency of security evaluations reflect any and all relevant federal or state laws? |
| **Primary References**<br><br><br><br><br><br>**Supplemental NIST References** | • NIST SP 800-26,*Security Self-Assessment Guide for Information Technology Systems*<br><br>• NIST SP800-53/FIPS 200, *Recommended Security Controls for Federal Information Systems*<br><br>• NIST SP800-14<br>• NIST SP800-37<br>• NIST SP800-55 | |

## Example 1:

A large hospital uses *Security Self-Assessment Guide for Information Technology Systems* (NIST SP 800-26) to evaluate its security practices. Responsibility is initially given to the IT Director, who forms a committee that includes the head of physical security, an executive in charge of legal and regulatory compliance, and administrative support staff. The IT Director modifies the Security Self-Assessment to reflect specific needs of the hospital, including the heightened security necessary for sensitive patient information, e.g., psychiatric records. In the information-gathering stage, the evaluation committee discovers that the responses to many questions vary according to department. Therefore the committee decides that some functions, such as granting access control, will be administered in a more centralized

way to ensure greater consistency and accountability for the process. This is one of the assessment's final recommendations.

### Example 2:

The director of a facility that performs diagnostic tests for physicians' offices and employers develops a checklist of security practices that includes all HIPAA Security requirements. While office staff members are researching the elements that this checklist should include, they realize that the facility's network security can be protected not only by the antivirus software it already uses, but also by firewalls. The firewalls will screen out other network traffic and provide the management of the facility with the ability to minimize inappropriate use of the Internet. The director of the facility develops an action plan to research, purchase, and train staff on using a firewall for the facility's IT system.

## 4.9 Business Associate Contracts and Other Arrangements (§164.308(b)(1))

**HIPAA Standard:** *A covered entity, in accordance with Sec. 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate appropriately safeguard the information.*

| Key Activities | Description | Sample Questions |
|---|---|---|
| | **Introductory Reference***: An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12 – Chapter 8)* | |
| **1. Identify Entities that Are Business Associates under the HIPAA Security Rule** | • Identify the individual or department who will be responsible for coordinating the execution of business associate agreements.<br>• Reevaluate the list of business associates to determine who has access to protected information to assess whether the list is complete and current.<br>• Identify systems covered by the contract/agreement. | • Do the business associate agreements written and executed contain sufficient language to ensure that required information types will be protected?<br>• Are there any new organizations or vendors that now provide a service or function on behalf of the organization? Such services may include the following:<br>– Claims processing or billing<br>– Data analysis<br>– Utilization review<br>– Quality assurance<br>– Benefit management<br>– Practice management<br>– Re-pricing<br>– All other HIPAA-regulated functions<br>– Hardware maintenance<br>Have outsourced functions involving the use of protected information been considered, such as the following:<br>– Actuarial services<br>– Data aggregation<br>– Administrative services<br>– Accreditation<br>– Financial services? |
| **2. Execute New Agreements or Update Existing Agreements as Appropriate** | • Identify roles and responsibilities.<br>• Include security requirements in business associate contracts/agreements to address confidentiality, integrity, and availability of sensitive information.<br>• Specify any training requirements associated with the contract/agreement. | • Who is responsible for coordinating and preparing the final agreement?<br>• Does the agreement specify how information is to be transmitted to and from the business associate?<br>• Does the agreement stipulate who is to have access to protected information and for what purpose? |
| **3. Establish Process for Measuring Contract Performance and Terminating the Contract if Security Requirements Are Not Being Met** | • Maintain clear lines of communication.<br>• Conduct security reviews.<br>• Establish criteria for measuring contract performance (metrics). | • What is the service being performed?<br>• What is the outcome expected?<br>• Is there a process for reporting security incidents related to the agreement?<br>• Is there a need to retain audit |

| | | |
|---|---|---|
| | | logs to support security reviews of the contract?<br>• Is there a process in place for terminating the contract if requirements are not being met and has the business associate been advised what conditions would warrant termination? |
| **Primary References**<br><br><br><br><br>**Supplemental NIST References** | • NIST SP 800-47,*Security Guide for Interconnecting Information Technology Systems*<br><br>• NIST SP 800-35,*Guide to Information Technology Security Services*<br><br>• NIST SP 800-14<br>• NIST SP 800-36<br>• NIST SP 800-53<br>• NIST SP 800-64 | |

### Example 1:

An organization that processes health care claims has decided to hire an IT vendor to provide system development and data center support services, including database support. Under this agreement, the vendor (a business associate) will have access to electronic health information. The organization, before finalizing the arrangement, prepares a set of security requirements that the vendor must address. These include access controls, audit logging and reporting, data backup and recovery, incident reporting, staff training, and hardware and software configuration. In addition, the agreement includes a stipulation that the organization can conduct security reviews of the vendor throughout the duration of the contract.

### Example 2:

A health care organization, as part of its fraud control program, has contracted with a third-party vendor to conduct a quality control study of Medicare claims to assess accuracy of billing. Because the vendor will have access to electronic health information in conducting the study, the organization includes extensive requirements for background checks, authentication, audit, and access controls in its contract language. It also includes specific requirements regarding the physical handling and storage of patient information while such information is in the vendor's possession.

## Physical Safeguards

### 4.10 Facility Access Controls (§164.310(A)(1))

**HIPAA Standard:** *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. (Note: Supports the Information Access Management Administrative Standard and the Access Control Technical Standard)*

| Key Activities | Description | Sample Questions |
|---|---|---|
| | **Introductory Reference:** *An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12 – Chapter 15)* | |
| **1. Conduct an Analysis of Existing Physical Security Vulnerabilities** | • Inventory facilities and identify shortfalls and/or vulnerabilities in current physical security capabilities.<br>• Assign degrees of significance to each vulnerability identified.<br>• Highest priority should be on the following primary types of facilities:<br>– Data Centers<br>– Peripheral equipment locations<br>– IT staff offices<br>– Workstation locations. | • Do nonpublic areas have locks and cameras?<br>• Are workstations protected from public access or viewing?<br>• Are entrances and exists secure?<br>• Do policies and procedures already exist regarding access to and use of facilities and equipment?<br>• What is the threat environment?<br>• Are there possible natural or man-made disasters that could happen in our environment?<br>• Do normal physical protections exist? (Locks on doors, windows, etc., and other means of preventing unauthorized access.) |
| **2. Identify Corrective Measures** | • Identify and assign responsibility for the measures and activities necessary to correct deficiencies.<br>• Develop and deploy policies and procedures to ensure that repairs, upgrades, and /or modifications are made to the appropriate physical areas of the facility. | • Who is responsible for security?<br>• Who is responsible for facility/physical security?<br>• Are policies and procedures already in place? Do they need to be revised?<br>• What training will be needed for employees to understand the policies and procedures?<br>• How will we document the decisions and actions?<br>• Are we dependent on a landlord to make physical changes to meet the requirements? |
| **3. Develop a Facility Security Plan** | • Document appropriate measures to provide physical security protection for EPHI in a covered entity's possession.<br>• Include documentation of the facility inventory, as well as information regarding the physical maintenance records and the history of changes, upgrades, and other modifications. | • Is there an inventory of facilities and existing security practices?<br>• What are the current procedures for securing the facilities (exterior, interior, equipment, access controls, maintenance records, etc.?<br>• Who is responsible for the facility plan?<br>• Is there a contingency plan already in place, under revision, or under development? |

| | | |
|---|---|---|
| **4. Develop Access Control Procedures** | • Develop policies and procedures to provide facility access to authorized personnel and visitors. | • What are the policies and procedures in place for controlling access by staff, contractors, visitors, and probationary employees?<br>• How many access points exist in each facility? Is there an inventory?<br>• Is monitoring equipment necessary? |
| **5. Establish Contingency Operations Procedures** | • Develop policies and procedures to provide appropriate facility access to emergency response personnel. | • Who needs access to the facility in the event of a disaster?<br>• What is the backup plan for facility access?<br>• Who is responsible for the contingency plan for the facility?<br>• Who is responsible for implementing the contingency plan in each department, unit, etc.?<br>• What is the backup plan for emergency access to EPHI?<br>• Have all types of potential disasters been considered (Fire, flood, earthquake, etc.)?<br>• Have clear lines of authority been established for crisis management-type decisions? |
| **Supplemental NIST References** | • NIST SP 800-14<br>• NIST SP 800-18<br>• NIST SP 800-26<br>• NIST SP 800-30<br>• NIST SP 800-34<br>• NIST SP 800-53 | |

### Example 1:

A three-physician office, with three additional staff, occupies an office suite in a building with other medical tenants. Access to the common areas of the building is controlled and managed adequately by the building's owner. The owner has additionally provided for barriers to be installed, preventing access through a false ceiling into and between individual office suites.

The office manager has developed a basic policy that specifies procedures for ensuring that locked doors and windows restrict access to electronic health information when the office is closed. During working hours, prevention of improper physical access is the responsibility of all office personnel, but primarily the office manager and receptionist. Due to the limited number of personnel involved, no special procedures were deemed necessary to ensure that authorized access be allowed. All personnel employed in the office are familiar with the contents of this policy.

### Example 2:

A large hospital, located in a major city has deemed it appropriate to emphasize security at all entrances and exits. This includes the use of numerous security cameras and guard personnel, 24 hours per day. Physical security requirements have been documented in the hospital's security and facilities plan, which

also assigns responsibility for facility security to the Security Official. IT facilities have been assigned priority levels for protection, with the highest level being assigned to the rooms housing the central processing function. A comprehensive contingency plan has been developed, and testing occurs at regular intervals.

## 4.11 Workstation Use (§164.310(b))

**HIPAA Standard:** *Implement 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 electronic protected health information.*

| Key Activities | Description | Sample Questions |
|---|---|---|
| | **Introductory Reference:** *An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12 – Chapters 15 & 16)* | |
| **1. Identify Workstation Types and Functions or Uses** | • Inventory workstations and devices.<br>• Develop policies and procedures for each type of workstation and workstation device, identifying and accommodating their unique issues (see note on workstations at the end of this section).<br>• Classify workstations based on the capabilities, connections, and allowable activities for each workstation used. | • Do we have an inventory of workstation types and locations in my organization?<br>• Who is responsible for this inventory and its maintenance?<br>• What tasks are commonly performed on a given workstation or type of workstation?<br>• Are there wireless tools in use as "workstations"? If so, what types and for what purpose? |
| **2. Identify Expected Performance of Each Type of Workstation** | • Develop and document policies and procedures related to the proper use and performance of workstations. | • How are workstations used in day-to-day operations?<br>• What are key operational risks that could result in a breach of security? |
| **3. Analyze Physical Surroundings for Physical Attributes** | • Ensure that any risks associated with a workstation's surroundings are known and analyzed for possible negative impacts.<br>• Develop policies and procedures that will prevent or preclude unauthorized access of unattended workstations, limit the ability of unauthorized persons to view sensitive information, and erase sensitive information as needed. | • Where are workstations located?<br>• Is viewing by unauthorized individuals restricted or limited at these workstations?<br>• Do changes need to be made in the space configuration?<br>• Do employees understand the security requirements for the data they use in their day-to-day jobs? |
| **Supplemental NIST References** | • NIST SP 800-14<br>• NIST SP 800-53 | |

### Example 1:

A hospital decides to standardize polices and procedures concerning the use of its workstations at nursing stations in wards throughout the facility. One of the elements common to these workstations is their physical surroundings. A policy has been issued that requires reasonable barriers to prevent unauthorized access or viewing by nonmedical personnel. These barriers would include counters and partitions, etc. Further, certain restrictions on what functions may be performed have been established for workstations deemed to be most vulnerable to viewing/access by unauthorized individuals.

### Example 2:

A small provider's office (one physician) has only two workstations in use, one of which is used solely for financial activities. The two office staff personnel are aware of what functions are to be performed on which workstation, and this information is documented. All personnel in the office have received information concerning proper security procedures by the receptionist, who maintains documentary evidence of this informal training process.

***Note***: The definition of workstation is an electronic computing device, i.e., desktop, laptop, or other device that performs similar functions, including the electronic media in its immediate environment. This latter statement extends the definition of workstation to a wider range of computer input and output devices—unintelligent and intelligent computer terminals, personal digital assistants, other wireless devices, diagnostic equipment, etc.

## 4.12 Workstation Security (§164.310(c))

**HIPAA Standard:** *Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.*

| Key Activities | Description | Sample Questions |
|---|---|---|
| | **Introductory Reference:** *An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12 - Chapter 15)* | |
| **1. Identify All Methods of Physical Access to Workstations** | • Document the different ways workstations are accessed by employees and nonemployees. | • Is there an inventory of all current workstation locations?<br>• Are any workstations located in public areas?<br>• Are laptops used as workstations? |
| **2. Analyze the Risk Associated with Each Type of Access** | • Determine which type of access holds the greatest threat to security. | • Are any workstations in areas that are more vulnerable to unauthorized use or viewing of the data they contain?<br>• What are the options for making modifications to the current access configuration? |
| **3. Identify Physical Safeguards** | • Document the options for deploying physical safeguards that will minimize the risk to security of electronic health information. | • What safeguards are in place i.e., locked doors, screen barriers, cameras, guards?<br>• Do any workstations need to be relocated to enhance physical security?<br>• Have employees been trained on security? |
| **Supplemental NIST References** | • NIST SP 800-14<br>• NIST SP 800-53 | |

### Example 1:

A rural hospital has established rules and procedures regarding physical access to workstations where electronic health information can be accessed. These safeguards include such requirements as keeping workstations out of public access areas (where possible), use of physical barriers to prevent inadvertent access, restricted viewing zones, and closed/locked doors. The facility is small enough to rule out the use of guard personnel as unreasonable. Special attention is given to workstations in areas or offices that are not manned 24 hours per day, with the standard procedure being a locked door as a minimum level of protection.

### Example 2:

A small provider's office has only two rooms where workstations are located. Both rooms are beyond the entrance door to the facility, and the office staff controls further access. One of the rooms housing workstations is not always staffed; therefore it is standard office policy to keep the door closed and locked.

## 4.13 Device and Media Controls (§164.310(d)(1))

**HIPAA Standard:** *Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.*

| Key Activities | Description | Sample Questions |
|---|---|---|
| | **Introductory Reference:** *An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12 – Chapter 14)* | |
| **1. Evaluate Methods for Final Disposal of Electronic Health Information (EPHI).** | • Determine and document the appropriate methods to dispose of hardware, software, and the data itself.<br>• Assure that EPHI is properly destroyed and cannot be recreated. | • What data is maintained by the organization, and where?<br>• Is data on removable, reusable media such as tapes and CDs?<br>• Is there a process for destroying data on hard drives and file servers?<br>• What are the options for disposing of data on hardware? What are the costs? |
| **2. Develop and Implement Procedures for reuse of electronic media** | • Ensure that health information previously stored on electronic media cannot be accessed and reused.<br>• Identify removable devices and their use.<br>• Ensure that EPHI is removed from reusable media before it is used to record new information. | • Do policies and procedures already exist regarding reuse of electronic media (hardware and software)<br>• Is one individual and/or department responsible for coordinating the disposal of data, and the reuse of the hardware and software?<br>• Are employees appropriately trained on security and risks to EPHI when reusing software and hardware? |
| **3. Maintain records of hardware, media, and personnel** | • Ensure that EPHI is not inadvertently released or shared with any unauthorized party.<br>• Ensure that an individual is responsible for, and records the receipt and removal of, hardware and software with EPHI. | • Where is data stored (what type of media)?<br>• What procedures already exist regarding tracking of hardware and software within the company?<br>• What procedures exist to track hardware and software externally?<br>• Who is responsible for maintaining records of hardware and software? |
| **4. Develop Backup procedures To ensure that the integrity of Electronic Health Information will not be jeopardized during equipment relocation** | • Ensure that an exact, retrievable copy of the data is retained and protected. | • Are backup files maintained offsite?<br>• Do backup procedures exist? Who has this responsibility?<br>• Are backup procedures documented and available to other staff?<br>• If data were to be unavailable for a period of time, what would the business impact be?<br>• Is there a contingency plan in place? |
| **Primary Reference** | • NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems* | |

| Key Activities | Description | Sample Questions |
|---|---|---|
| **Supplemental NIST References** | • NIST SP 800-34<br>• NIST SP 800-53 | |

### Example 1:

A health plan has established organization wide policies and procedures for device and media control. Equipment capable of storing electronic health information may only be disposed of by the Information Security department, which will ensure that appropriate technical measures are taken to prevent unauthorized access to stored information. Both equipment and storage media that are destined for reuse will be routed through the same Information Security department before being transferred for the same purpose. Proper employment of backup procedures will be verified for all equipment relocations.

### Example 2:

A small provider's office has instituted policies that address the control of removable storage media from workstations. At present this only includes floppy discs, but provisions have been incorporated into the guidance to cover newer, high-capacity storage devices. Basically, these policies require that removable media be protected by locked storage devices when not in use and specify procedures to be taken in the event that a workstation must be removed from the office to protect the confidentiality of information. These policies may include the establishment of maintenance agreements requiring appropriate background checks, the signing of nondisclosure agreements, physical escorts, etc.

## Technical Safeguards

### 4.14 Access Controls (§164.312(a)(1))

**HIPAA Standard:** *Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4). (Note: Supports the Information Access Management Administrative Standard and Facility Access Controls Physical Standard)*

| Key Activities | Description | Sample Questions |
|---|---|---|
| | **Introductory Reference:** *An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12 – Chapter 17)* | |
| **1. Analyze Workloads and Operations To Identify the Access Needs of All Users** | • Identify an approach for access control.<br>• Consider all applications and systems containing electronic health information that should only be available to approved users. | • What are the applications/systems that require access controls?<br>• What user roles are defined for those applications/systems?<br>• Where is the health information supporting those applications/systems currently housed (e.g, stand-alone PC, network)?<br>• Are data and/or systems being accessed remotely? |
| **2. Identify All Data and Systems Where Access Control Is a Requirement** | • Determine the scope and degree of access control needed. | • How are the systems accessed (viewing data, modifying data, creating data)?<br>• Are passwords being used?<br>• If so, are they unique by individual? |
| **3. Ensure that All System Users Have Been Assigned a Unique Identifier** | • Ensure that system activity can be traced to a specific user.<br>• Ensure that the necessary data is available in the system logs to support audit and other related business functions. | • How should the identifier be established (length and content)?<br>• Should the identifier be self-selected or randomly generated?<br>• How often should the identifier be changed? |
| **4. Develop Access Control Policy** | • Establish a formal policy for access control that will guide the development of procedures.<br>• Specify requirements for access control that are both feasible and cost-effective for implementation. | • Have rules of behavior been established and communicated to system users?<br>• How will rules of behavior be enforced?<br>• Has a determination been made on use of encryption? |
| **5. Implement Access Control Procedures Using Selected Hardware and Software** | • Implement the policy and procedures using a cost-effective hardware/software solution. | • Who will manage the access controls procedures?<br>• Are current users trained in access control management?<br>• Will user training be needed to implement access control procedures? |
| **6. Review and Update User Access** | • Enforce policy and procedures as a matter of ongoing operations.<br>• Determine if any changes are needed for access control | • Have new employees/users been given proper instructions for protecting data and systems?<br>• What are the procedures for new |

| | | |
|---|---|---|
| | mechanisms.<br>• Establish procedures for updating access when users require the following:<br>– Initial access<br>– Increased access<br>– Access to different systems or applications than those they currently have. | employee/user access to data and systems?<br>• Are there procedures for reviewing and, if appropriate, modifying access authorizations for existing users? |
| **7. Establish an Emergency Access Procedure** | • Identify a method of supporting continuity of operations should the normal access procedures be disabled or unavailable due to system problems. | • When should the emergency access procedure be activated?<br>• Who is authorized to make the decision?<br>• Who has assigned roles in the process?<br>• Is the emergency access procedure to be a default emergency procedure, which has been established and communicated to all users, or is it a process restricted to, and conducted by, a few authorized individuals?<br>• Can it be activated on a user- by-user basis? |
| **8. Terminate Access if it Is No Longer Required** | • Ensure only those with a need to know have access to protect data and systems. | • Are rules being enforced to remove access by staff members who no longer have a need to know because they have changed assignments or have stopped working for the organization? |
| **Supplemental NIST References** | • NIST SP 800-14<br>• NIST SP 800-53<br>• NIST SP 800-56<br>• NIST SP 800-57<br>• NIST SP 800-63<br>• FIPS 140-2 | |

### Example 1:

A hospital is concerned that patient data can be accessed from computers that are located in an open area. The policy is implemented that after five minutes of nonuse, the computer automatically launches the screensaver, preventing user access. Upon return, the user must logon with an assigned password.

### Example 2:

In a small health care provider organization, many users (managers, assistants, nurses, health care professionals, clerical users) have access to systems for general activities. For certain very sensitive information, only a few users have access to the information in the system. The office has assigned individual IDs to all users for general access and has assigned special passwords to those individuals having access to very sensitive information.

## 4.15 Audit Controls (§164.312(b))

**HIPAA Standard:** *Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.*

| Key Activities | Description | Sample Questions |
|---|---|---|
| | **Introductory Reference:** *An Introduction to Computer Security: The NIST Handbook (NIST Special Publication 800-12 – Chapter 18)* | |
| **1. Determine the Systems or Activities that Will Be Tracked or Audited** | • Determine the appropriate scope of any system audits that will be necessary based on the size and needs of the covered entity.<br>• Use results of risk assessment to determine which systems and activities should be tracked and audited<br>• Determine what data needs to be captured. | • Where is EPHI at risk in the organization?<br>• What systems, applications, or processes make data vulnerable to unauthorized or inappropriate tampering, uses, or disclosures?<br>• What activities will be monitored (Create, Read, Update, Delete = CRUD)?<br>• What should the audit record include (e.g., user ID, event type/date/time)? |
| **2. Select the Tools that Will Be Deployed for Auditing and System Activity Reviews** | • Evaluate existing system capabilities and determine if any changes or upgrades are necessary. | • What tools are in place?<br>• What are the most appropriate monitoring tools for our organization (third party, freeware, or operating system-provided)?<br>• Are changes/upgrades cost effective? |
| **3. Develop and Deploy the Information System Activity Review/Audit Policy** | • Document and communicate to the workforce the facts about the organization's decisions on audits and reviews. | • Who is responsible for the overall audit process and results?<br>• How often will audits take place?<br>• How often will audit results be analyzed?<br>• What is the organization's sanction policy for employee violations?<br>• Where will audit information reside (i.e., separate server)? |
| **4. Develop Appropriate Standard Operating Procedures** | • Determine the types of audit trail data and monitoring procedures that will be needed to derive exception reports. | • How will exception reports or logs be reviewed?<br>• Where will monitoring reports be filed and maintained?<br>• Is there a formal process in place to address system misuse, abuse, and fraudulent activity?<br>• How will managers and employees be notified, when appropriate, regarding suspect activity? |
| **5. Implement the Audit/System Activity Review Process** | • Activate the necessary audit system<br>• Begin logging and auditing procedures. | • What mechanisms will be implemented to assess the effectiveness of the audit process (metrics)?<br>• What is the plan to revise the audit process when needed? |

| Key Activities | Description | Sample Questions |
|---|---|---|
| **NOTE:** | • The descriptions and questions/tasks that appear in this module assume that the appropriate policies have been written and that the Security Official, the Security Management Plan and infrastructure are in place. | |
| **Supplemental NIST References** | • NIST SP 800-14<br>• NIST SP 800-53 | |

### Example 1:

In a small health care provider organization, the policy is that any queries against a patient's record by employees must be related to that employee's assigned work. To check this control, an audit process has been put in place to perform a daily match of individual employee queries against cases assigned. An Exception Report is generated for the operational manager if there is no match, and follow-up with the employee is conducted.

### Example 2:

A hospital is very concerned that patient information residing on the hospital network could be compromised by insider misuse in collusion with information brokers (scams where unauthorized, external parties may attempt to gain access to health care information by trickery or bribery). In response to this concern, the director of the hospital has implemented an audit process, which runs against daily network logs looking for employee access patterns that fall outside of normal baselines (query volumes) for daily query activity within the employee's job category of interest. These cases are written to a file for later review and follow-up.

## 4.16 Integrity (§164.312(c)(1))

**HIPAA Standard:** *Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.*

| Key Activities | Description | Sample Questions |
|---|---|---|
| | **Introductory Reference:** *An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12 – Chapter 5)* | |
| **1. Identify All Users Who Have Been Authorized to Access Electronic-Protected Health Information** | • Identify all approved users with the ability to alter or destroy data<br>• Address this Step in conjunction with the identification of unauthorized sources in Step 2, below. | • How are users authorized to access the information? (See **Access Control** standard.)<br>• Is there a sound basis established as to why they need the access?<br>• Have they been trained on how to use the information?<br>• Is there an audit trail established for all accesses to the information? (See **Audit** standard.) |
| **2. Identify Any Possible Unauthorized Sources that May Be Able to Intercept the Information and Modify it** | • Identify scenarios that may result in modification to the electronic health information by unauthorized sources (e.g., hackers, disgruntled employees, business competitors)<br>• Consider conducting this activity as part of your Risk Analysis (See Security Management Process Standard, Step 2.) | • What are likely sources that could jeopardize information integrity?<br>• What can be done to protect the integrity of the information when it is residing on a system (at rest)?<br>• What procedures and policies can be established to decrease or eliminate alteration of the information during transmission (e.g., encryption)?<br>• How feasible and cost-effective for our environment are the options being considered? |
| **3. Develop the Integrity Policy and Requirements** | • Establish a formal (written) set of integrity requirements based on the results of the analysis completed in the previous steps. | • Have the requirements been discussed and agreed to by identified key personnel involved in the processes that are affected?<br>• Have the requirements been documented?<br>• Has a written policy been developed and communicated to system users? |
| **4. Implement Procedures to Address These Requirements** | • Identify which methods will be used to protect the information from modification.<br>• Identify tools and techniques to be developed or procured that support the assurance of integrity. | • Are current audit, logging, and access control techniques sufficient to address the integrity of the information?<br>• If not, what additional techniques can we apply to check information integrity (e.g., quality control process, transaction and output reconstruction)?<br>• Can additional training of users decrease instances attributable to human errors? |

| | | |
|---|---|---|
| **5. Establish a Monitoring Process To Assess How the Implemented Process Is Working** | • Review existing processes to determine if objectives are being addressed<br>• Reassess integrity processes continually as technology and operational environments change to determine if they need to be revised. | • Are there reported instances of information integrity problems and have they decreased since integrity procedures have been implemented?<br>• Does the process, as implemented, provide a higher level of assurance that information integrity is being maintained? |
| **Primary Reference**<br><br>**Supplemental NIST References** | • NIST SP 800-14,*Generally Accepted Principles and Practices for Securing Information Technology Systems*<br><br>• NIST SP 800-42<br>• NIST SP 800-44<br>• NIST SP 800-53 | |

### Example 1:

A support vendor has been experiencing a high number of complaints from the health care provider it supports regarding errors in the health care information housed in the database, creating an ongoing integrity issue. The health care provider reports an unacceptably high degree of errors in conversion of the hardcopy input into a record contained in the vendor's database file. The health care provider has requested that steps be taken to decrease the high error rate, which it attributes to inexperienced workers in the vendor's operation. The vendor has responded that much of the input being submitted is illegible, leading to errors during data entry. To address both concerns, the support vendor has offered to develop a series of online input templates that apply some surface editing (e.g., ensuring that an input field meets certain requirements such as type [numeric, alphabetic, alphanumeric] and length [9 digits, 8 letters, etc.]). The support vendor and the health care provider have agreed to monitor the process during the next 90 days to see if the problem is be resolved.

### Example 2:

A small health care provider keeps its electronic health information on a personal computer in the office. The personal computer does have an Internet connection. Once a month, the manager of the office uses this computer to transmit the entire patient file to a third-party support vendor for offsite backup. To address possible integrity attacks on the information, the office manager has installed a personal firewall and uses encryption for the monthly transmission. Office personnel also routinely update the computer's antivirus software to avoid loss or modification of the data through a virus attack.

## 4.17 Person or Entity Authentication (§164.312(d))8

**HIPAA Standard:** *Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.*

| Key Activities | Description | Sample Questions |
|---|---|---|
| | **Introductory Reference:** *An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12- Chapter 16)* | |
| **1. Determine Authentication Applicability to Current Systems/Applications** | • Identify methods available for authentication. Authentication is the process of establishing the validity of a transmission source or verifying an individual's authorization claim for specific access privileges to information and information systems. | • What authentication methods are available?<br>• What are the advantages and disadvantages of each method?<br>• What will it cost to implement the available methods in our environment?<br>• Do we have trained staff who can maintain the system or do we need to consider outsourcing some of the support? |
| **2.Evaluate Authentication Options Available** | • Weigh the relative advantages and disadvantages of commonly used authentication approaches.<br>• There are four commonly used authentication approaches available:<br>– Something a person knows, such as a password,<br>– Something a person has or is in possession of, such as a token (smart card, ATM card, etc.),<br>– Some type of biometric identification a person provides, such as a fingerprint, or<br>– A combination of two or more of the above approaches. | • What are the strengths and weaknesses of each available option?<br>• Which can be best supported with assigned resources (budget/staffing)?<br>• What level of authentication is appropriate based on our assessment of risk to the information/systems?<br>• Do we need to acquire outside vendor support to implement the process? |
| **3.Select and Implement Authentication Option** | • Consider the results of the analysis conducted under Step 2, above, and select appropriate authentication methods.<br>• Implement the methods selected into your operations and activities. | • Has necessary user and support staff training been completed?<br>• Have formal authentication policy and procedures been established and communicated?<br>• Has necessary testing been completed to ensure that the authentication system is working as prescribed?<br>• Do the procedures include ongoing system maintenance and updates?<br>• Is the process implemented in such a way that it does not compromise the authentication |

[8] Note: This standard is supported by both the access control and audit control standards.

| | | |
|---|---|---|
| | | information (password file encryption, etc.) |
| **Supplemental NIST References** | • NIST SP 800-14<br>• NIST SP 800-53<br>• NIST SP 800-63 | |

### Example 1:

Customers are allowed to call an 800 number to get the status of their health care transactions. To receive the information over the telephone, the provider requires that they give an account number and in addition provide responses to several "knowledge-based" questions. If they cannot provide the information, the information requested is not made available, and an exception record is written to the log file, which is used for followup by internal auditors.

### Example 2:

A large health care provider has an extensive network of support vendors and system users. Many of the online transactions involve disclosure of health care information. The provider needs to address many things, including ensuring that information disclosures are made to the correct individuals and/or organizations. To address this requirement, the health care provider has implemented the use of hardware tokens (smart cards) for authentication.

### Example 3:

A large pharmaceutical company must transmit transactions to a government agency for assessment. To identify itself and ensure that the government agency can trust the source, the pharmaceutical company has obtained a Public Key Infrastructure (PKI) certificate and has decided to digitally sign all transactions submitted to the government agency.

## 4.18 Transmission Security (§164.312(e)(1))

**HIPAA Standard:** *Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.*

| Key Activities | Description | Sample Questions: |
|---|---|---|
| | **Introductory Reference:** *An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12 – Chapter 16 &19)* | |
| **1. Identify Any Possible Unauthorized Sources that May Be Able to Intercept and/or Modify the Information** | • Identify scenarios that may result in modification to the electronic protected health information (EPHI) by unauthorized sources during transmission (e.g., hackers, disgruntled employees, business competitors). | • What measures exist to protect EPHI?<br>• What measures are planned to protect EPHI?<br>• Is there an auditing process in place?<br>• Is there assurance that information is not altered during transmission?<br>• Are there trained staff members to monitor transmissions? |
| **2. Develop a Transmission Security Policy** | • Establish a formal (written) set of requirements for transmitting electronic protected health information. | • Have the requirements been discussed and agreed to by identified key personnel involved in transmitting electronic health information?<br>• Has a written policy been developed and communicated to system users? |
| **3. Implement Procedures for Transmitting Electronic Health Information Using Hardware/Software if Needed** | • Identify methods of transmission that will be used to protect electronic health information<br>• Identify tools and techniques that will be used to support the transmission security policy. | • Is encryption needed to effectively protect the information?<br>• Is encryption feasible and cost-effective in this environment?<br>• Are staff members skilled in the use of encryption? |
| **Supplemental NIST References** | • NIST SP 800-14<br>• NIST SP 800-42<br>• NIST SP 800-53<br>• NIST SP 800-63<br>• FIPS 140-2 | |

### Example 1:

A health care provider has decided to use the Internet to transmit patient data to a support vendor for backup and contingency operations. The transmission of this data should be protected from disclosure. No one who is not authorized to read the file should be able to monitor the transmission and capture the information during its transmission. The health care provider has decided to design and implement a web application, which enforces the use of strong encryption methods to prevent unauthorized disclosure of the data during transmission.

# Appendix A—References[9]

## Public Laws

Public Law 107-347, E-Government Act of 2002 (Title III: Federal Information Security Management Act (FISMA) of 2002), December 17, 2002.

Public Law 104-191, Health Insurance Portability and Accountability Act (HIPAA) of 1996, August 21, 1996.

## Federal Regulations

Health Insurance Reform: Security Standards; Final Rule ("The HIPAA Security Rule"), 68 FR 8334, February 20, 2003.

OMB Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting,* August 6, 2003.

## Federal Information Processing Standards (FIPS) Publications

FIPS 140-2, *Security Requirements for Cryptographic Modules,* June 2001.

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems,* February 2004.

## National Institute of Standards and Technology (NIST) Guidelines

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook,* October 1995.

NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996.

NIST SP 800-16, *Information Technology Security Training Requirements: A Role- And Performance-Based Mode*l April 1998.

NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems,* December 1998.

NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems,* November 2001.

NIST SP 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security),* January 2004.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems,* January 2002.

NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems,* June 2002.

NIST SP 800-35, *Guide to Information Technology Security Services,* October 2003.

[9] Status and most current versions of the NIST documents (Draft or Final) can be found at http://csrc.nist.gov/publications.

NIST SP 800-36, *Guide to Selecting Information Security Products,* October 2003.

NIST 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* April 2004.

NIST SP 800-42, *Guideline on Network Security Testing,* October 2003.

NIST SP 800-44, *Guidelines on Securing Public Web Servers,* September 2002.

NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems,* September 2002.

NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program,* October 2003.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems,* October 2003.

***Note**: Eventually this publication will become FIPS 200.*

NIST SP 800-55, *Security Metrics Guide for Information Technology Systems,* July 2003.

NIST SP 800-56, *Recommendation on Key Establishment Schemes,* January 2003.

NIST SP 800-57, *Recommendation on Key Management,* January 2003.

NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System,* August 2003.

NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories,* March 2004.

NIST SP 800-61, *Computer Security Incident Handling Guide,* January 2004.

NIST SP 800-63, *Recommendation for Electronic Authentication,* January 2004.

NIST SP 800-64, *Security Considerations in the Information Systems Development Life Cycle,* October 2003.

### Web sites and Other Resources

National Institute of Standards and Technology (NIST): Computer Security Resource Center (CSRC): http://csrc.nist.gov/

Department of Health and Human Services (DHHS), Centers for Medicare and Medicaid Services (CMS), HIPAA Resources: http://www.cms.hhs.gov/hipaa/

Workgroup for Electronic Data Interchange (WEDI): http://www.wedi.org

National Committee on Vital and Health Statistics (NCVHS): http://ncvhs.hhs.gov

## Appendix B—Glossary

The terms and definitions used in this Special Publication (SP) have been obtained from Congressional legislation, executive orders, Office of Management and Budget (OMB) policies, and commonly accepted glossaries of security terminology, including that of National Institute of Standards and Technology (NIST) SP 800-53, *Recommended Security Controls for Federal Information Systems*.

| | |
|---|---|
| **Administrative Safeguards** [45 Code of Federal Regulations (C.F.R.) Sec. 160.304] | Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic health information and to manage the conduct of the covered entity's workforce in relation to protecting that information. |
| **Addressable** | As applied to an implementation specification of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), describing a measure that is mandatory for all HIPAA-covered entities unless the entity concludes the measure is not "reasonable and appropriate" after conducting a required analysis. The covered entity may still be required to implement an equivalent measure if the equivalent measure is "reasonable and appropriate" and achieves the same end as the addressable implementation specification. |
| **Affiliated Covered Entities** [45 C.F.R. Sec. 164.105] | Legally separated covered entities that are under common ownership or control and that have all designated themselves as single affiliated covered entities for the purposes of the Privacy and Security Rule (more precisely, those parts of the Rules appearing at 45 CFR, Part 160, Subparts C and E). |
| **Availability** [45 C.F.R. Sec. 160.304] | The property that data or information is accessible and usable on demand by an authorized person. |
| **Business Associate** [45 C.F.R. Sec. 160.103] | An entity independent of a HIPAA-covered entity that handles individually identifiable health information received from or provided to the covered entity. For examples of the kinds of activities conducted by business associates, as well as certain exceptions to the definition, see Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82462 (2000) at 82798. |
| **Computer Security Contingency** [NIST SP 800-12] | An event with the potential to disrupt computer operations, thereby disrupting critical mission and business functions, for example, a power outage, hardware failure, fire, or storm. If the event is very destructive, it is often called a **disaster.** |
| **Confidentiality** [45 C.F.R. Sec. 164.304] | The property that data or information is not made available or disclosed to unauthorized persons or processes. |

| | |
|---|---|
| **Contingency** | See **Computer Security Contingency.** |
| **Controls** | See **Security Controls.** |
| **Countermeasures** | Synonymous with security controls and safeguards. |
| **Covered Entities**<br>[45 C.F.R. Sec.160.103] | Entities that must comply with any or all of the HIPAA Rules in this document, including certain providers, health plans, and health care clearinghouses that are regulated by the HIPAA Security Rule and/or the HIPAA Privacy Rule. |
| **Electronic Protected Health Information (EPHI)**<br>[45 C.F.R. Sec.160.103] | Individually identifiable health information (IIHI) that is transmitted or maintained electronically. EPHI excludes information transmitted or maintained in media that are not electronic. Some other categories of information included in "IIHI" are excluded by EPHI such as some educational and employment records. |
| **Final Rule** | The version of the specific requirements for compliance with a statute published by the agency empowered to do so by the relevant statute. Final Rules are published after a public comment period and are usually redrafted to account for issues identified by these public comments. The Final Security and Privacy Rules set compliance deadlines, after which they are effective and enforceable. |
| **Health Care Clearinghouse**<br>[45 C.F.R. Sec.160.103] | A public or private entity that processes or facilitates the processing of health information received from another entity to or from a standard format. |
| **Health Care Provider**<br>[45 C.F.R. Sec. 160.103] | A provider of medical or health services and any other person who furnishes, bills, or is paid for health care in the normal course of business. |
| **Health Information**<br>[45 C.F.R. Sec. 160.103] | Any information, whether oral or recorded in any form or medium, that that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment of the provision of health care to an individual. |
| **Health Plan**<br>[45 C.F.R. Sec.160.103] | An individual or group plan that provides or pays the cost of medical care. |

| | |
|---|---|
| **Hybrid Entity**<br>[45 C.F.R. Sec.164.103] | A single legal entity that is a covered entity, whose business activities include both covered and non-covered functions, and that has designated one or more of its components as health care components in accordance with 45 CFR section 164.105(a)(2)(iii)(C). |
| **Impact** | See **Potential Impact.** |
| **Implementation Specification**<br>[45 C.F.R. Sec. 160.103] | Specific requirements or instructions for implementing a standard. |
| **Individually Identifiable Health Information (IIHI)**<br>[45 C.F.R. Sec. 160.103] | Information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse, and relates to the past, present, or future physical or mental health of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. |
| **Information Security**<br>[44 U.S.C., Sec. 3542] | The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, integrity, and availability. |
| **Information System**<br>[44 U.S.C., Sec. 3502] | A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. |
| **Information Technology** | Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. |
| **Integrity**<br>[45 C.F.R. Sec. 160.304] | The property that data or information has not been altered or destroyed in an unauthorized manner. |
| **Management Controls** | The security controls (i.e., safeguards and countermeasures) applied to an information system that focus on the management of risk and the management of the information security system. Actions that are performed primarily to support management decisions with regard to information system security. |

| | |
|---|---|
| **Measures** | See **Security Controls.** |
| **Mitigate** | See **Risk Mitigation**. |
| **National Security Information** | Information that has been determined pursuant to Executive Order 12958 or any predecessor order, or by the Atomic Energy Act of 1954 as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status. |
| **National Security System** [44 U.S.C., Sec. 3542] | Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which—involves intelligence activities, involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. |
| **Operational Controls** | The security controls (i.e., safeguards and countermeasures) applied to an information system that are primarily implemented and executed by people (as opposed to the information system). |
| **Potential Impact [FIPS 199]** | Low: The loss of confidentiality, integrity, or availability could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals. Moderate: The loss of confidentiality, integrity, or availability could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals. High: The loss of confidentiality, integrity, or availability could be expected to have a *severe* or *catastrophic* adverse effect on organizational operations, organizational assets, or individuals. |
| **Physical Safeguards** | Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion. See Health Insurance Reform: Security Standards; Final Rule 68 Fed. Reg. 8334 (2003), at 8376 (to be codified at 45 C.F.R. section 164.304). |

| | |
|---|---|
| **Proposed Rule** | Proposed requirements for compliance with a statute that is published for public comment by the agency empowered to do so by the relevant statute. Proposed rules are not binding (e.g., covered entities will not be subject to penalty for not complying with a proposed rule). |
| **Protected Health Information (PHI)** | Individually identifiable health information that is transmitted or maintained electronically or by using any other medium. Some categories of information included in "IIHI" are not considered to be EPHI, such as some educational and employment records. See Health Insurance Reform: Security Standards; Final Rule 68 Fed. Reg. 8334 (2003), at 8376 (to be codified at 45 C.F.R. section 160.103). |
| **Required** | Mandatory—as applied to a HIPAA implementation specification—for all covered entities to comply with HIPAA Rules. |
| **Risk**<br>**[NIST SP 800-30, Rev A]** | The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the probability of that threat occurring. |
| **Risk Mitigation**<br>**[NIST SP 800-12]** | The selection and implementation of security controls to reduce risk to a level acceptable to management, within applicable constraints. |
| **Safeguards** | Synonymous with security controls and countermeasures. |
| **Security** | See **Information Security.** |
| **Security Controls** | The management, operational, and technical controls (safeguards or countermeasures) prescribed for an information system and the security controls in place or planned for meeting those requirements. |
| **Standard** | A rule, condition, or requirement that must be met by a covered entity. See Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82462 (2000) at 82800 (to be codified at 45 C.F.R. section 160.103). |

| | |
|---|---|
| **Technical Safeguards** | The security controls (i.e., safeguards and countermeasures) applied to an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. |
| **Threat**<br>**[NIST SP 800-30]** | The potential for a threat source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability. |
| **Threat Source**<br>**[NIST SP 800-30]** | Either (1) intent and method targeted at the intentional exploitation of a vulnerability, or (2) a situation and method that may accidentally trigger a vulnerability. |
| **User** | An individual or organization granted access to an information system. |
| **Vulnerability** | A flaw or weakness in the design or implementation of an information system (including the security procedures and security controls associated with the system) that could be intentionally or unintentionally exploited to adversely affect an organization's operations or assets through a loss of confidentiality, integrity, or availability. |

## Appendix C—Acronyms

The appendix lists acronyms used within this document.

| | |
|---|---|
| **C.F.R.** | Code of Federal Regulations |
| **CIO** | Chief Information Officer |
| **CMS** | Centers for Medicare and Medicaid Services |
| **CSD** | Computer Security Division |
| **CSRC** | Computer Security Resource Center |
| **EPHI** | Electronic Protected Health Information |
| **FedCIRC** | Federal Computer Incident Response Center |
| **FISMA** | Federal Information Security Management Act of 2002 |
| **FIPS PUBS** | Federal Information Processing Standards Publications |
| **HHS** | Department of Health and Human Services |
| **HIPAA** | Health Insurance Portability and Accountability Act of 1996 |
| **ID** | Identification |
| **IIHI** | Individually Identifiable Health Information |
| **ISP** | Internet Service Provider |
| **IT** | Information Technology |
| **ITL** | Information Technology Laboratory |
| **LAN** | Local Area Network |
| **NIST** | National Institute of Standards and Technology |
| **OIG** | Office of the Inspector General |
| **OMB** | Office of Management and Budget |
| **PHI** | Protected Health Information |
| **PKI** | Public Key Infrastructure |
| **SP** | Special Publication |
| **U.S.C.** | United States Code |
| **U.S.** | United States |

## Appendix D—HIPAA Security Rule/NIST Publications Crosswalk[10]

This appendix provides a matrix that crosswalks the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule to available National Institute of Standards and Technology (NIST) publications that readers may draw upon for consideration in implementing the Security Rule.

**Table D-1. HIPAA Security Rule/NIST Publications Crosswalk**

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | NIST Publications |
|---|---|---|
| **Administrative Safeguards** | | |
| 164.308(a)(1)(i) | **Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.** | **NIST SP 800-12,** *An Introduction to Computer Security: The NIST Handbook,* October 1995.<br>**NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996.<br>**NIST SP 800-18,** *Guide For Developing Security Plans For Information Technology Systems,* December 1998.<br>**NIST SP 800-26,** *Security Self-Assessment Guide for Information Technology Systems, November 2001.*<br>***NIST SP 800-27,*** *Engineering Principles for Information Technology Security (A Baseline for Achieving Security),* January 2004.<br>**NIST SP 800-30,** *Risk Management Guide to Information Technology Systems,* January 2004.<br>**NIST SP 800-37,** *Guide for the Security Certification and Accreditation of Federal Information Systems,* April 2004.<br>**NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems,* October 2003.<br>**NIST SP 800-60,** *Guide for Mapping Types of Information and Information Systems to Security Categories,* Fall 2003.<br>**FIPS 199,** *Standards for Security Categorization of Federal Information and Information Systems,* February 2004. |
| 164.308(a)(1)(ii)(A) | Risk Analysis (R): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity. | |
| 164.308(a)(1)(ii)(B) | Risk Management (R): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | |
| 164.308(a)(1)(ii)(C) | Sanction Policy (R): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. | |
| 164.308(a)(1)(ii)(D) | Information System Activity Review (R): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | |
| 164.308(a)(2) | **Assigned Security Responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.** | **NIST SP 800-12,** *An Introduction to Computer Security: The NIST Handbook,* October 1995.<br>**NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996.<br>**NIST SP 800-26,** *Security Self-Assessment Guide for Information Technology Systems,* November 2001.<br>**NIST SP 800-53**. *Recommended Securitv* |

[10] Status and most current versions of the NIST documents (Draft or Final) can be found at http://csrc.nist.gov/publications.

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | NIST Publications |
|---|---|---|
| | | *Controls for Federal Information Systems,* October 2003. |
| 164.308(a)(3)(i) | **Workforce Security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.** | **NIST SP 800-12,** *An Introduction to Computer Security: The NIST Handbook,* October 1995.<br>**NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996.<br>**NIST SP 800-26,** *Security Self-Assessment Guide for Information Technology Systems,* November 2001.<br>**NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems,* October 2003. |
| 164.308(a)(3)(ii)(A) | Authorization and/or Supervision (A): Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | |
| 164.308(a)(3)(ii)(B) | Workforce Clearance Procedure (A): Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | |
| 164.308(a)(3)(ii)(C) | Termination Procedure (A): Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section. | |
| 164.308(a)(4)(i) | **Information Access Management: Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.** | **NIST SP 800-12,** *An Introduction to Computer Security: The NIST Handbook,* October 1995.<br>**NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996.<br>**NIST SP 800-18,** *Guide For Developing Security Plans for Information Technology Systems,* December 1998.<br>**NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems,* October 2003.<br>**NIST SP 800-63,** *Recommendation for Electronic Authentication,* January 2004. |
| 164.308(a)(4)(ii)(A) | Isolating Health Care Clearinghouse Function (R): If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | |
| 164.308(a)(4)(ii)(B) | Access Authorization (A): Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | |

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | NIST Publications |
|---|---|---|
| 164.308(a)(4)(ii)(C) | Access Establishment and Modification (A): Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | |
| 164.308(a)(5)(i) | **Security Awareness and Training: Implement a security awareness and training program for all members of its workforce (including management).** | **NIST SP 800-12,** *An Introduction to Computer Security: The NIST Handbook,* October 1995.<br>**NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996.<br>**NIST SP 800-16,** *Information Technology Security Training Requirements: A Role- and Performance-Based Model,* April 1998.<br>**NIST SP 800-50,** *Building an Information Technology Security Awareness and Training Program,* October 2003.<br>**NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems*, October 2003. |
| 164.308(a)(5)(ii)(A) | Security Reminders (A): Implement periodic security updates. | |
| 164.308(a)(5)(ii)(B) | Protection from Malicious Software (A): Implement Procedures for guarding against, detecting, and reporting malicious software. | |
| 164.308(a)(5)(ii)(C) | Login Monitoring (A): Implement procedures for monitoring login attempts and reporting discrepancies. | |
| 164.308(a)(5)(ii)(D) | Password Management (A): Implement procedures for creating, changing, and safeguarding passwords. | |
| 164.308(a)(6)(i) | **Security Incident Procedures: Implement policies and procedures to address security incidents.** | **NIST SP 800-12,** *An Introduction to Computer Security: The NIST Handbook,* October 1995.<br>**NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996.<br>**NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems,* October 2003.<br>**NIST SP 800-61,** *Computer Security Incident Handling Guide,* January 2004. |
| 164.308(a)(6)(ii) | Response and Reporting (R): Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. | |
| 164.308(a)(7)(i) | **Contingency Plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.** | **NIST SP 800-12,** *An Introduction to Computer Security: The NIST Handbook,* October 1995.<br>**NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996.<br>**NIST SP 800-18,** *Guide For Developing Security Plans For Information Technology Systems,* December 1998.<br>**NIST SP 800-26,** *Security Self-Assessment Guide for Information Technology Systems,* November 2001.<br>**NIST SP 800-30,** *Risk Management Guide to Information Technology Systems, January 2004.* |
| 164.308(a)(7)(ii)(A) | Data Backup Plan (R): Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | |
| 164.308(a)(7)(ii)(B) | Disaster Recovery Plan (R): Establish (and implement as needed) procedures to restore any loss of data. | |

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | NIST Publications |
|---|---|---|
| 164.308(a)(7)(ii)(C) | Emergency Mode Operation Plan (R): Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | **NIST SP 800-34,** *Contingency Planning Guide for Information Technology Systems,* June 2002.<br>**NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems,* October 2003. |
| 164.308(a)(7)(ii)(D) | Testing and Revision Procedure (A): Implement procedures for periodic testing and revision of contingency plans. | |
| 164.308(a)(7)(ii)(E) | Applications and Data Criticality Analysis (A): Assess the relative criticality of specific applications and data in support of other contingency plan components. | |
| 164.308(a)(8) | **Evaluation: Perform a periodic technical and non technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.** | **NIST SP 800-12,** *An Introduction to Computer Security: The NIST Handbook,* October 1995.<br>**NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996.<br>**NIST SP 800-26,** *Security Self-Assessment Guide for Information Technology Systems,* November 2001.<br>**NIST SP 800-37,** *Guide for the Security Certification and Accreditation of Federal Information Systems,* April 2004.<br>**NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems,* October 2003.<br>**NIST SP 800-55,** *Security Metrics Guide for Information Technology Systems,* July 2003. |
| 164.308(b)(1) | **Business Associate Contracts and Other Arrangements: A covered entity, in accordance with Sec. 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only of the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate appropriately safeguard the information.** | **NIST SP 800-12,** *An Introduction to Computer Security: The NIST Handbook,* October 1995.<br>**NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996.<br>**NIST SP 800-35,** *Guide to Information Technology Security Services,* October 2003.<br>**NIST SP 800-36,** *Guide to Selecting Information Security Products,* October 2003.<br>**NIST SP 800-47,** *Security Guide for Interconnecting Information Technology Systems,* September 2002.<br>**NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems,* October 2003.<br>**NIST SP 800-64,** *Security Considerations in the Information System Development Life Cycle,* October 2003. |
| 164.308(b)(4) | Written Contract or Other Arrangement (R): Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of Sec. 164.314(a). | |

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | NIST Publications |
|---|---|---|
| **Physical Safeguards** | | |
| 164.310(a)(1) | **Facility Access Controls: 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.** | **NIST SP 800-12,** *An Introduction to Computer Security: The NIST Handbook,* October 1995.<br>**NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996.<br>**NIST SP 800-18,** *Guide For Developing Security Plans For Information Technology Systems,* December 1998.<br>**NIST SP 800-26,** *Security Self-Assessment Guide for Information Technology Systems,* November 2001.<br>**NIST SP 800-30,** *Risk Management Guide to Information Technology Systems,* January 2004.<br>**NIST SP 800-34,** *Contingency Planning Guide for Information Technology Systems,* June 2002.<br>**NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems,* October 2003. |
| 164.310(a)(2)(i) | Contingency Operations (A): Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. | |
| 164.310(a)(2)(ii) | Facility Security Plan (A): Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. | |
| 164.310(a)(2)(iii) | Access Control and Validation Procedures (A): Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. | |
| 164.310(a)(2)(iv) | Maintenance Records (A): Implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for example, hardware, walls, doors, and locks). | |
| 164.310(b) | **Workstation Use: Implement 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 electronic protected health information.** | **NIST SP 800-12,** An Introduction to Computer Security: The NIST Handbook, October 1995.<br>**NIST SP 800-14,** Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996.<br>**NIST SP 800-53,** Recommended Security Controls for Federal Information Systems, October 2003. |
| 164.310(c) | **Workstation Security: Implement physical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.** | **NIST SP 800-12,** An Introduction to Computer Security: The NIST Handbook, October 1995.<br>**NIST SP 800-14,** Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996.<br>**NIST SP 800-53,** Recommended Security Controls for Federal Information Systems, October 2003. |

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | NIST Publications |
|---|---|---|
| 164.310(d)(1) | **Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.** | **NIST SP 800-12,** An Introduction to Computer Security: The NIST Handbook, October 1995.<br>**NIST SP 800-14,** Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996.<br>**NIST SP 800-34,** Contingency Planning Guide for Information Technology Systems, June 2002.<br>**NIST SP 800-53,** Recommended Security Controls for Federal Information Systems, October 2003. |
| 164.310(d)(2)(i) | Disposal (R): Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored. | |
| 164.310(d)(2)(ii) | Media Re-Use (R): Implement procedures for removal of electronic protected health information from electronic media before the media are made available for reuse. | |
| 164.310(d)(2)(iii) | Accountability (A): Maintain a record of the movements of hardware and electronic media and any person responsible therefore. | |
| 164.310(d)(2)(iv) | Data Backup and Storage (A): Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment. | |
| **Technical Safeguards** | | |
| 164.312(a)(1) | **Access Controls: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).** | **NIST SP 800-12,** An Introduction to Computer Security: The NIST Handbook, October 1995.<br>**NIST SP 800-14,** Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996.<br>**NIST SP 800-53,** Recommended Security Controls for Federal Information Systems, October 2003.<br>**NIST SP 800-56,** Recommendation on Key Establishment Schemes, January 2003.<br>**NIST SP 800-57,** Recommendation on Key Management, January 2003.<br>**NIST SP 800-63,** Recommendation for Electronic Authentication, January 2004.<br>**FIPS 140-2,** Security Requirements for Cryptographic Modules, June 2001. |
| 164.312(a)(2)(i) | Unique User Identification (R): Assign a unique name and/or number for identifying and tracking user identity. | |
| 164.312(a)(2)(ii) | Emergency Access Procedure (R): Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. | |
| 164.312(a)(2)(iii) | Automatic Logoff (A): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. | |
| 164.312(a)(2)(iv) | Encryption and Decryption (A): Implement a mechanism to encrypt and decrypt electronic protected health information. | |
| 164.312(b) | **Audit Controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected** | **NIST SP 800-12,** An Introduction to Computer Security: The NIST Handbook, October 1995.<br>**NIST SP 800-14,** Generally Accepted Principles and Practices for Securing Information |

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | NIST Publications |
|---|---|---|
| | **health information**. | Technology Systems, September 1996.<br>**NIST SP 800-53,** Recommended Security Controls for Federal Information Systems, October 2003. |
| 164.312(c)(1) | **Integrity: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.** | **NIST SP 800-12,** An Introduction to Computer Security: The NIST Handbook, October 1995.<br>**NIST SP 800-14,** Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996.<br>**NIST SP 800-42,** Guideline on Network Security Testing, October 2003.<br>**NIST SP 800-44,** Guidelines on Securing Public Web Servers, *September 2002.*<br>**NIST SP 800-53,** Recommended Security Controls for Federal Information Systems, *October 2003.* |
| 164.312(c)(2) | Mechanism to Authenticate Electronic Protected Health Information (A): Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. | |
| 164.312(d) | **Person or Entity Authentication: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.** | **NIST SP 800-12,** An Introduction to Computer Security: The NIST Handbook, October 1995.<br>**NIST SP 800-14,** Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996.<br>**NIST SP 800-53,** Recommended Security Controls for Federal Information Systems, October 2003.<br>**NIST SP 800-63,** Recommendation on Electronic Authentication, January 2004. |
| 164.312(e)(1) | **Transmission Security: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.** | **NIST SP 800-12,** An Introduction to Computer Security: The NIST Handbook, October 1995.<br>**NIST SP 800-14,** Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996.<br>**NIST SP 800-42,** Guideline on Network Security Testing, October 2003.<br>**NIST SP 800-53,** Recommended Security Controls for Federal Information Systems, October 2003.<br>**NIST SP 800-63,** Recommendation for Electronic Authentication, January 2004.<br>**FIPS 140-2,** *Security Requirements for Cryptographic Modules,* June 2001. |
| 164.312(e)(2)(i) | Integrity Controls (A): Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | |
| 164.312(e)(2)(ii) | Encryption (A): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | |

## Appendix E—HIPAA Security Rule/FISMA Requirements Crosswalk

This appendix provides a crosswalk of the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule to the requirements of the Federal Information Security Management Act of 2002 (FISMA), which contains requirements relevant to the security programs of all Federal agencies.

**Table E-1. HIPAA Security Rule/FISMA Requirements Crosswalk**

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | Relevant FISMA Provisions[11] | Intersection |
|---|---|---|---|
| **ADMINISTRATIVE SAFEGUARDS** | | | |
| 164.308(a)(1)(i) | **Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.** | **Ref §3544(a)(b)(1)** "Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency." | HIPAA and FISMA require evaluation or implementation of similar safeguards. |
| 164.308(a)(1)(ii)(A) | Risk Analysis (R): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity. | **Ref §3544(a)(b)(1)** "Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency." | HIPAA and FISMA require evaluation or implementation of similar safeguards |
| 164.308(a)(1)(ii)(B) | Risk Management (R): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | **Ref §3544(b)(2)** "policies and procedures that—(A) are based on the risk assessments required by paragraph (1);(B) cost-effectively reduce information security risks to an acceptable level; (C) ensure that information security is addressed throughout the life cycle of each agency information system; and (D) ensure compliance with—(i) the requirements of this subchapter; (ii) | HIPAA and FISMA require evaluation or implementation of similar safeguards |

[11] In addition to NIST 800-26, specifically mentioned in OMB Memorandum M-03-19, NIST SP 800-53 also includes a set of controls that are required by FISMA and that are relevant to the security controls addressed in the Table E-1 above.

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | Relevant FISMA Provisions[11] | Intersection |
|---|---|---|---|
| | | policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40; (iii) minimally acceptable system configuration requirements, as determined by the agency; and (iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President...." | |
| 164.308(a)(1)(ii)(C) | Sanction Policy (R): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. | **NIST SP 800-26, Appendix A** "Personnel Security: … 6.1.5 Are mechanisms in place for holding users responsible for their actions?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |
| 164.308(a)(1)(ii)(D) | Information System Activity Review (R): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | **NIST SP 800-26, Appendix A** "Data Integrity: 11.2.5. Are intrusion detection tools installed on the system? 11.2.6 Are the intrusion detection reports routinely reviewed and suspected incidents handled accordingly? 11.2.7 Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks?" "Audit Trails: 17.1 Critical Element: Is activity involving access to a modification of sensitive or critical files logged, monitored, and possible security violations investigated? 17.1.1 Does the audit trail provide a trace of user actions?...17.1.2. Can the audit trail support after-the-fact investigations of how, when, and why normal operations ceased? 17.1.6. Are audit trails reviewed frequently?...17.1.7. Are automated tools used to review audit records in real time or near real time?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | Relevant FISMA Provisions[11] | Intersection |
|---|---|---|---|
| 164.308(a)(2) | **Assigned Security Responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.** | **Ref §3544(a)(3)** "delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this sub-chapter, including—''(A) designating a senior agency information security officer...." | HIPAA and FISMA require evaluation or implementation of similar safeguards. |
| 164.308(a)(3)(i) | **Workforce Security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.** | **NIST SP 800-26, Appendix A** "Personnel Security: 6.1.8 Is there a process for requesting, establishing, issuing, and closing user accounts?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (Aug 6, 2003). |
| 164.308(a)(3)(ii)(A) | Authorization and/or Supervision (A): Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | **NIST SP 800-26, Appendix A** "Personnel Security: … 6.1 Critical Element: Are duties separated to ensure least privilege and individual accountability? … 6.1.2 Are there documented job descriptions that accurately reflect assigned duties and responsibility and that segregate duties?...6.1.5 Are mechanisms in place for holding users responsible for their actions?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |
| 164.308(a)(3)(ii)(B) | Workforce Clearance Procedure (A): Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | **NIST SP 800-26, Appendix A** "Personnel Security: … 6.2 Critical Element: Is appropriate background screening for assigned positions completed prior to granting access? 6.2.1 Are individuals who are authorized to bypass significant technical and operational controls screened prior to access and periodically thereafter? 6.2.2 Are confidentiality or security agreements required for employees assigned to work with sensitive information? 6.2.3 When controls cannot adequately protect the information, are individuals screened prior to access? | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | Relevant FISMA Provisions[11] | Intersection |
|---|---|---|---|
| | | 6.2.4 Are there conditions for allowing system access prior to completion of screening?" | |
| 164.308(a)(3)(ii)(C) | Termination Procedure (A): Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section. | **NIST SP 800-26, Appendix A** "Personnel Security: … 6.1.7. Are hiring, transfer, and termination procedures established? 6.1.8 Is there a process for requesting, establishing, issuing, and closing user accounts?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |
| 164.308(a)(4)(i) | **Information Access Management: Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.** | **Ref §3544(b)(2)** "policies and procedures that—(A) are based on the risk assessments required by paragraph (1);(B) cost-effectively reduce information security risks to an acceptable level; (C) ensure that information security is addressed throughout the life cycle of each agency information system; and (D) ensure compliance with—(i) the requirements of this subchapter; (ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40; (iii) minimally acceptable system configuration requirements, as determined by the agency; and (iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President...." | HIPAA and FISMA require evaluation or implementation of similar safeguards. |
| 164.308(a)(4)(ii)(A) | Isolating Health Care Clearinghouse Function (R): If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | **NIST SP 800-26, Appendix A** "Risk Management: 1.1.1 Is the current system configuration documented, including links to other systems?" "Review of Security Controls: 2.1 Critical Element: Have the security controls of the system and interconnected systems been reviewed?" "Authorize Processing (C&A): 4.1.8 Has management authorized interconnections to all systems (including systems owned and operated by another program, agency, organization, or | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | Relevant FISMA Provisions[11] | Intersection |
|---|---|---|---|
| | | contractor)?" "Hardware and System Software Maintenance: 10.1.4 Is the operating system configured to prevent circumvention of the security software and application controls?" "Identification and Authentication: 15.1 Critical Element: Are users individually authenticated via passwords, tokens, or other devices?" | |
| 164.308(a)(4)(ii)(B) | Access Authorization (A): Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | **NIST SP 800-26, Appendix A** "Identification and Authentication: 15.1 Critical Element: Are users individually authenticated via passwords, tokens, or other devices? 15.1.1 Is a current list maintained and approved of authorized users and their access?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |
| 164.308(a)(4)(ii)(C) | Access Establishment and Modification (A): Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | **NIST SP 800-26, Appendix A** "Identification and Authentication: 15.1 critical Element: Are users individually authenticated via passwords, tokens, or other devices? 15.1.1 Is a current list maintained and approved of authorized users and their access?" "Logical Access Controls: 16.1 Critical Element: Do the logical access controls restrict users to authorized transactions and functions? 16.1.1. Can the security controls detect unauthorized access attempts?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |
| 164.308(a)(5)(i) | **Security Awareness and Training: Implement a security awareness and training program for all members of its workforce (including management).** | **Ref §3544(b)(4)** "security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—(A) information security risks associated with their activities; and (B) their responsibilities in complying with agency policies and procedures designed to reduce these risks...." | HIPAA and FISMA require evaluation or implementation of similar safeguards. |

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | Relevant FISMA Provisions[11] | Intersection |
|---|---|---|---|
| 164.308(a)(5)(ii)(A) | Security Reminders (A): Implement periodic security updates. | **NIST SP 800-26, Appendix A** "Security Awareness, Training, and Education: 13.1.3 Is there mandatory annual refresher training? 13.1.4 Are methods employed to make employees aware of security, i.e., posters, booklets?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |
| 164.308(a)(5)(ii)(B) | Protection from Malicious Software (A): Implement Procedures for guarding against, detecting, and reporting malicious software. | **NIST SP 800-26, Appendix A** "Data Integrity: 11.1 Critical Element: Is virus detection and elimination software installed and activated? 11.1.1 Are virus signature files routinely updated? 11.1.2 Are virus scans automatic?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |
| 164.308(a)(5)(ii)(C) | Login Monitoring (A): Implement procedures for monitoring login attempts and reporting discrepancies. | **NIST SP 800-26, Appendix A** "Logical Access Controls: 16.1 Critical Element: Do the logical access controls restrict users to authorized transactions and functions? 16.1.1 Can the security controls detect unauthorized access attempts? … 16.1.10 Is access monitored to identify apparent security violations and are such events investigated?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |
| 164.308(a)(5)(ii)(D) | Password Management (A): Implement procedures for creating, changing, and safeguarding passwords. | **NIST SP 800-26, Appendix A** "Identification and Authentication: 15.1 Critical Element: Are users individually authenticated via passwords, tokens, or other devices?…Are passwords changed at least every ninety days or earlier of needed? 15.1.7 Are passwords unique and difficult to guess (e.g., do passwords require alpha numeric, upper/lower case, and special characters)? 10 Are there procedures in place for handling lost and compromised passwords? | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | Relevant FISMA Provisions[11] | Intersection |
|---|---|---|---|
| | | 15.1.11 Are passwords distributed securely and users informed not to reveal their passwords to anyone (social engineering)?" | |
| 164.308(a)(6)(i) | **Security Incident Procedures: Implement policies and procedures to address security incidents.** | **Ref §3544(b)(7)** "procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued pursuant to section 3546(b), including—(A) mitigating risks associated with such incidents before substantial damage is done; (B) notifying and consulting with the Federal information security incident center referred to in section 3546; and (C) notifying and consulting with, as appropriate—(i) law enforcement agencies and relevant Offices of Inspector General; (ii) an office designated by the President for any incident involving a national security system; and (iii) any other agency or office, in accordance with law or as directed by the President...." | HIPAA and FISMA require evaluation or implementation of similar safeguards. |
| 164.308(a)(6)(ii) | Response and Reporting (R): Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. | **Ref §3544(b)(7)** "procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued pursuant to section 3546(b), including—"(A) mitigating risks associated with such incidents before substantial damage is done; (B) notifying and consulting with the Federal information security incident center referred to in section 3546; and (C) notifying and consulting with, as appropriate—'(i) law enforcement agencies and relevant Offices of Inspector General;' (ii) an office designated by the President for any incident involving a national security system; and (iii) any other agency or office, in accordance with law or as directed by the President..." | HIPAA and FISMA require evaluation or implementation of similar safeguards. |
| 164.308(a)(7)(i) | **Contingency Plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health** | **Ref §3544(b)(8)** "...plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency." | HIPAA and FISMA require evaluation or implementation of similar safeguards. |

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | Relevant FISMA Provisions[11] | Intersection |
|---|---|---|---|
| | **information.** | | |
| 164.308(a)(7)(ii)(A) | Data Backup Plan (R): Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | **NIST SP 800-26, Appendix A** "Contingency Planning: … 9.1.1 Are critical data files and operations identified and the frequency of file backup documented? … 9.2.5 Is the location of stored backups identified? …Are backup files created on a prescribed basis and rotated offsite often enough to avoid disruption if current files are damaged?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |
| 164.308(a)(7)(ii)(B) | Disaster Recovery Plan (R): Establish (and implement as needed) procedures to restore any loss of data. | **Ref §3544(b)(8)** "...plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency." | HIPAA and FISMA require evaluation or implementation of similar safeguards. |
| 164.308(a)(7)(ii)(C) | Emergency Mode Operation Plan (R): Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | **Ref §3544(b)(8)** "...plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency." | HIPAA and FISMA require evaluation or implementation of similar safeguards. |
| 164.308(a)(7)(ii)(D) | Testing and Revision Procedure (A): Implement procedures for periodic testing and revision of contingency plans. | **NIST SP 800-26, Appendix A** "Contingency Planning: 9.3 Critical Element: Are tested contingency/disaster recovery plans in place? … 9.3.3 Is the plan periodically tested and readjusted as appropriate?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |
| 164.308(a)(7)(ii)(E) | Applications and Data Criticality Analysis (A): Assess the relative criticality of specific applications and data in support of other contingency plan components. | **NIST SP 800-26, Appendix A** "Contingency Planning: 9.1 Critical Element: Have the most critical and sensitive operations and their supporting computer resources been identified? … 9.1.1 Are critical data files and operations identified and the frequency of file backup documented?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, |

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | Relevant FISMA Provisions[11] | Intersection |
|---|---|---|---|
| | | | 2003). |
| 164.308(a)(8) | **Evaluation: Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.** | **Ref §3544(b)(6)** "a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency." **Ref §3545(a)(1)** "Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices." | HIPAA and FISMA require evaluation or implementation of similar safeguards. |
| 164.308(b)(1) | **Business Associate Contracts and Other Arrangements: A covered entity, in accordance with Sec. 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate appropriately safeguard the information.** | **Ref §3544(a)(1)(A)(ii)** states that the head of each agency shall be responsible for "...information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency" | HIPAA and FISMA require evaluation or implementation of similar safeguards. |
| 164.308(b)(4) | Written Contract or Other Arrangement (R): Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of Sec. 164.314(a). | **NIST 800-26, Appendix A** "Contingency Planning: 9.1 Critical Element: Have the most critical and sensitive operations and their supporting computer resources been identified? … 9.1.1 Are critical data files and operations identified and the frequency of file backup documented?" "Authorize Processing (C&A): 4.1.8 Has management authorized interconnections to all systems (including systems owned and operated by another program, agency, organization, or contractor)?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | Relevant FISMA Provisions[11] | Intersection |
|---|---|---|---|
| **Physical Safeguards** | | | |
| 164.310(a)(1) | **Facility Access Controls: 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.** | **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate" **Ref §3544(b)(8)** "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency." | HIPAA and FISMA require evaluation or implementation of similar safeguards. |
| 164.310(a)(2)(i) | Contingency Operations (A): Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. | **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate." **Ref §3544(b)(8)** "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency." | HIPAA and FISMA require evaluation or implementation of similar safeguards. |
| 164.310(a)(2)(ii) | Facility Security Plan (A): Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. | **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate." **Ref §3544(b)(8)** "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency." | HIPAA and FISMA require evaluation or implementation of similar safeguards. |
| 164.310(a)(2)(iii) | Access Control and Validation Procedures (A): Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. | **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate." **Ref §3544(b)(8)** "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency." | HIPAA and FISMA require evaluation or implementation of similar safeguards. |
| 164.310(a)(2)(iv) | Maintenance Records (A): Implement policies and procedures to document repairs and modifications to the physical components of a facility, which that are related to security (for example, hardware, walls, doors, and locks). | **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate" AND **Ref §3544(b)(8)** "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency." | HIPAA and FISMA require evaluation or implementation of similar safeguards. |
| 164.310(b) | **Workstation Use: Implement policies and procedures that specify the proper functions to** | **Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and | HIPAA and FISMA require evaluation or implementation of similar safeguards. |

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | Relevant FISMA Provisions[11] | Intersection |
|---|---|---|---|
| | **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 electronic protected health information.** | magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate." | |
| 164.310(c) | **Workstation Security: Implement physical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.** | **Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate." | HIPAA and FISMA require evaluation or implementation of similar safeguards. |
| 164.310(d)(1) | **Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.** | **Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate." | HIPAA and FISMA requirements require evaluation or implementation of similar safeguards. |

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | Relevant FISMA Provisions[11] | Intersection |
|---|---|---|---|
| 164.310(d)(2)(i) | Disposal (R): Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored. | **NIST SP 800-26, Appendix A** "Disposal Phase: 3.2.11 Are official electronic records properly disposed/archived?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |
| 164.310(d)(2)(ii) | Media Re-Use (R): Implement procedures for removal of electronic protected health information from electronic media before the media are made available for reuse. | **NIST 800-26, Appendix A** "Disposal Phase: 3.2.12 Is information or media purged, overwritten, degaussed, or destroyed when disposed or used elsewhere?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |
| 164.310(d)(2)(iii) | Accountability (A): Maintain a record of the movements of hardware and electronic media and any person responsible therefore. | **NIST SP 800-26, Appendix A** "Disposal Phase:... 3.2.13 Is a record kept of who implemented the disposal actions and verified that the information or media was sanitized?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |
| 164.310(d)(2)(iv) | Data Backup and Storage (A): Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment. | **NIST SP 800-26, Appendix A** "Contingency Planning: … 9.1.1 Are critical data files and operations identified and the frequency of file backup documented? … 9.2.5 Is the location of stored backups identified? … Are backup files created on a prescribed basis and rotated offsite often enough to avoid disruption if current files are damaged?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | Relevant FISMA Provisions[11] | Intersection |
|---|---|---|---|
| **Technical Safeguards** | | | |
| 164.312(a)(1) | **Access Controls: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).** | **Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate." | HIPAA and FISMA requirements require evaluation or implementation of similar safeguards. |
| 164.312(a)(2)(i) | Unique User Identification (R): Assign a unique name and/or number for identifying and tracking user identity. | **NIST SP 800-26, Appendix A** "Identification and Authentication: 15.1 Critical Element: Are users individually authenticated via passwords, tokens, or other devices?…Are passwords changed at least every ninety days or earlier if needed? 15.1.7 Are passwords unique and difficult to guess (e.g., do passwords require alpha numeric, upper/lower case, and special characters)?" "Logical Access Controls: 16.1.10 Is access monitored to identify apparent security violations and are such events investigated?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |
| 164.312(a)(2)(ii) | Emergency Access Procedure (R): Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. | **NIST SP 800-26, Appendix A** "Identification and Authentication: 15.1.4 Is emergency and temporary access authorized?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | Relevant FISMA Provisions[11] | Intersection |
|---|---|---|---|
| 164.312(a)(2)(iii) | Automatic Logoff (A): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. | **NIST SP 800-26, Appendix A** "Logical Access Controls: 16.1.4 Do workstations disconnect or screensavers lock system after a specific period of inactivity?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |
| 164.312(a)(2)(iv) | Encryption and Decryption (A): Implement a mechanism to encrypt and decrypt electronic protected health information. | **Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate."<br>**NIST SP 800-26, Appendix A** "Logical Access Controls: 16.1.7 If encryption is used, does it meet Federal standards? 16.1.8 If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving? ...16.2.14 Are sensitive data transmissions encrypted?" | HIPAA and FISMA requirements require evaluation or implementation of similar safeguards; specific standards are required if encryption is deemed necessary and implemented |
| 164.312(b) | **Audit Controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.** | **Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an | HIPAA and FISMA requirements require evaluation or implementation of similar safeguards. |

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | Relevant FISMA Provisions[11] | Intersection |
|---|---|---|---|
| | | agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate." | |
| 164.312(c)(1) | **Integrity: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.** | **Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate." | HIPAA and FISMA requirements require evaluation or implementation of similar safeguards. |
| 164.312(c)(2) | Mechanism to Authenticate Electronic Protected Health Information (A): Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. | **NIST SP 800-26, Appendix A** "Data Integrity: 11.2 Critical Element: Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended? 11.2.1 Are reconciliation routines used by applications, i.e., checksums, hash totals, record counts? 11.2.4 Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions? ... 11.2.9 Is message authentication used?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |
| 164.312(d) | **Person or Entity Authentication: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.** | **Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or | HIPAA and FISMA requirements require evaluation or implementation of similar safeguards. |

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | Relevant FISMA Provisions[11] | Intersection |
|---|---|---|---|
| | | groups of information systems, as appropriate." | |
| 164.312(e)(1) | **Transmission Security: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.** | **Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate." | HIPAA and FISMA requirements require evaluation or implementation of similar safeguards. |
| 164.312(e)(2)(i) | Integrity Controls (A): Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | **NIST SP 800-26, Appendix A** "Data Integrity: 11.2 Critical Element: Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended? 11.2.1 Are reconciliation routines used by applications, i.e., checksums, hash totals, record counts? 11.2.4 Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions? ... 11.2.9 Is message authentication used?" | Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003). |
| 164.312(e)(2)(ii) | Encryption (A): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | **Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate."<br>**NIST SP 800-26, Appendix A** | HIPAA and FISMA requirements require evaluation or implementation of similar safeguards; specific standards are required if encryption is deemed necessary and implemented |

| Section of HIPAA Security Rule | HIPAA Safeguard (R) = Required (A) = Addressable | Relevant FISMA Provisions[11] | Intersection |
|---|---|---|---|
| | | "Logical Access Controls: 16.1.7 If encryption is used, does it meet federal standards? 16.1.8 If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving? ...16.2.14 Are sensitive data transmissions encrypted?" | |