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

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

INFORMATION SECURITY

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

March 2005

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

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

National Institute of Standards and Technology
Hratch G. Semerjian, Jr., Acting 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 other than 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, the Secretary of Health and Human Services, 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 would like to thank all of those who assisted in reviewing working drafts of this document as well as those who participated in related workshops and meetings and provided their comments to assist in developing this special publication.

Disclaimer

This publication is intended as general guidance only for federal organizations, and is not intended to be, nor should it be construed or relied upon as legal advice or guidance to non-federal entities or persons. This document does not modify the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or any other federal law or regulation. The participation of other federal organizations with the National Institute of Standards and Technology (NIST) and NIST workgroups in the development of this special publication does not, and shall not be deemed to, constitute the endorsement, recommendation, or approval by those organizations of its contents.

TABLE OF CONTENTS

Executive Summary

Some federal agencies, in addition to being subject to the Federal Information Security Management Act of 2002 (FISMA), are also subject to similar requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule (the Security Rule), if the agency is a covered entity as defined by the rules implementing HIPAA.

This Special Publication summarizes the HIPAA security standards and explains some of the structure and organization of the Security Rule. This publication helps to educate readers about information security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security standards set out in the Security Rule. This publication is also designed to direct 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. 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 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 their functions and use of EPHI. All HIPAA covered entities, which include some federal agencies, must comply with the Security Rule. The Security Rule specifically focuses on protecting the confidentiality, integrity, and availability of EPHI, as defined in the Security Rule. The EPHI that a covered entity creates, receives, maintains, or transmits must be protected against reasonably anticipated threats, hazards, and impermissible uses and/or disclosures. In general, the requirements, standards, and implementation specifications of the Security Rule apply to the following covered entities:

- Covered Health Care Providers—Any provider of medical or other health services, or supplies, who transmits any health information in electronic form in connection with a transaction for which HHS has adopted a standard.
- Health Plans—Any individual or group plan that provides, or pays the cost of, medical care, including certain specifically listed governmental programs (e.g., a health insurance issuer and the Medicare and Medicaid programs).
- Health Care Clearinghouses—A public or private entity that processes another entity's health care transactions from a standard format to a non-standard format, or vice-versa.
- Medicare Prescription Drug Card Sponsors –A nongovernmental entity that offers an endorsed discount drug program under the Medicare Modernization Act. This fourth category of "covered entity" will remain in effect until the drug card program ends in 2006.

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 are information security programs in place and trained personnel assigned to manage and support the programs. Heavy emphasis is placed on fully integrating security into the business processes. Preparation of security plans and certification and accreditation (C&A) 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 help 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

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 and effectiveness of information technology (IT) planning, implementation, management, and operation.

NIST publishes a wide variety of 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 are the security standards adopted by the Secretary of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Public Law 104-191). HIPAA required the Secretary to adopt, among other standards, security standards for certain 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 publications were cited as potentially valuable resources to readers with specific questions and concerns about IT security.

Congress enacted the Administrative Simplification (part of Title II) provisions of HIPAA to, among other things, promote efficiency in the health care industry through the use of standardized electronic transactions, while protecting the privacy and security of health information. Pursuant to the Administrative Simplification provisions of HIPAA, the Secretary of HHS adopted standards relating to:

- Electronic healthcare transactions and code sets;
- Privacy of protected health information;
- Security of electronic protected health information (EPHI); and
- Unique health identifiers.

This Special Publication summarizes the HIPAA security standards and explains some of the structure and organization of the Security Rule. This publication helps to educate readers about information security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security standards set out in the Security Rule. This publication is also designed to direct 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. 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 HIPAA Security Rule itself. While CMS mentioned several of these publications in the preamble to the HIPAA Security Rule, CMS does not require their use in complying with the Security Rule.[1]

This document addresses only the security standards of the Security Rule and not other provisions adopted or raised by the Rule, such as 45 CFR § 164.105.

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

[1] The HIPAA Security Rule mentions NIST documents as potentially helpful guidance but not mandatory for compliance, at 68 *Federal Register* pages 8346, 8350, 8352, and 8355 (February 20, 2003).

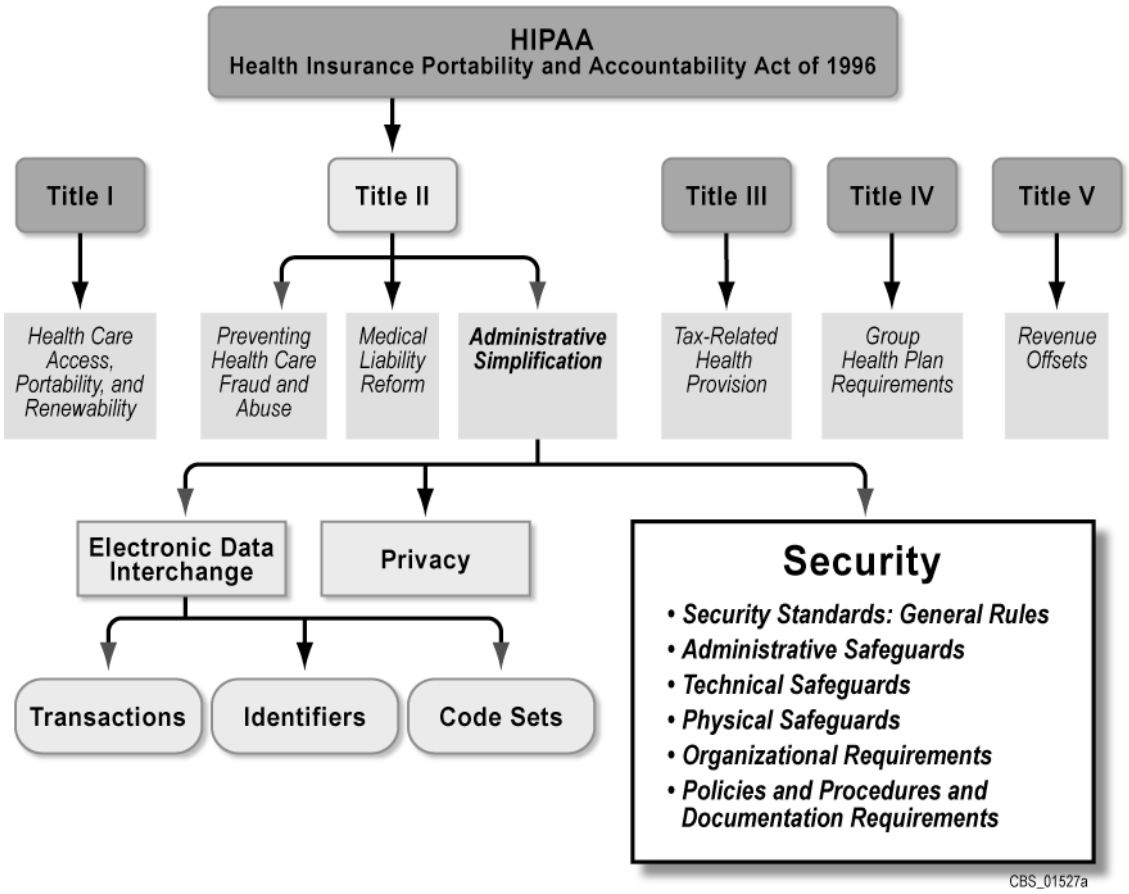

Figure 1. HIPAA Components

"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.[2] Readers should 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 HIPAA 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 publication is to help educate readers about the security standards included in the HIPAA Security Rule. This document is also designed to direct readers to helpful information in other NIST publications on security topics included in the HIPAA Security Rule. Readers can draw upon these publications for consideration in implementing the Security Rule.

The guidance provided in this publication is applicable to all federal information systems,[3] other than those systems designated as national security systems as defined in 44 United States Code (U.S.C.),

[2] The definition of "small health plan" at 45 CFR § 160.103 applies to all of the HIPAA rules, including the Security Rule. A "small" health plan is one with annual receipts of $5 million or less.

[3] 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.

Section 3542.[4] The guidance included in this publication has been broadly developed from a technical perspective 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 health infrastructure of the United States are encouraged to consider using these guidelines, as appropriate.

NIST publications may be useful to any agency seeking to understand the security issues raised by the HIPAA Security Rule regardless of that agency's size, structure, or distribution of security responsibilities. Specific agency missions, resources, and organizational structures, however, vary greatly, and agencies' approaches to implementing the HIPAA Security Rule may diverge significantly. Federal agencies use different titles to identify roles that have security-related responsibilities and may also assign 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.

The preamble of the Security Rule states that HHS does not rate or endorse the use of industry developed guidelines and/or models. Organizations that are not required to use this NIST special publication (by other regulation, law, or requirement), yet choose to use it, must determine the value of its content for implementing the Security Rule standards in their environments. The use of this publication or any other NIST publication does not ensure or guarantee an organization will be compliant with the Security Rule.

1.2 Scope

This publication provides a brief overview of the HIPAA Security Rule, directs the reader to additional NIST publications on information security, and identifies typical activities an agency should consider in implementing an information security program.

This publication is intended as an aid for federal agencies to understand security concepts discussed in the HIPAA Security Rule and does not supplement, replace, modify 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.

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.

[4] 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 or 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 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.

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.

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

Section 4 maps NIST publications to the standards that describe the HIPAA Security Rule's administrative, technical, physical security controls, general administrative, and organizational requirements.

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 Computer Security Division (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 by an agency 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[5]

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 an 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	*Electronic Authentication Guide: Recommendations of the National Institute of Standards and Technology*
NIST SP 800-64	*Security Considerations in the Information System Development Life Cycle*
NIST SP 800-65	*Integrating Security into the Capital Planning and Investment Control Process*

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

2.1 Security Program Development Life Cycle

The phases of a typical security program life cycle can be used to assist an organization with addressing the standards of the HIPAA Security Rule. 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 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.

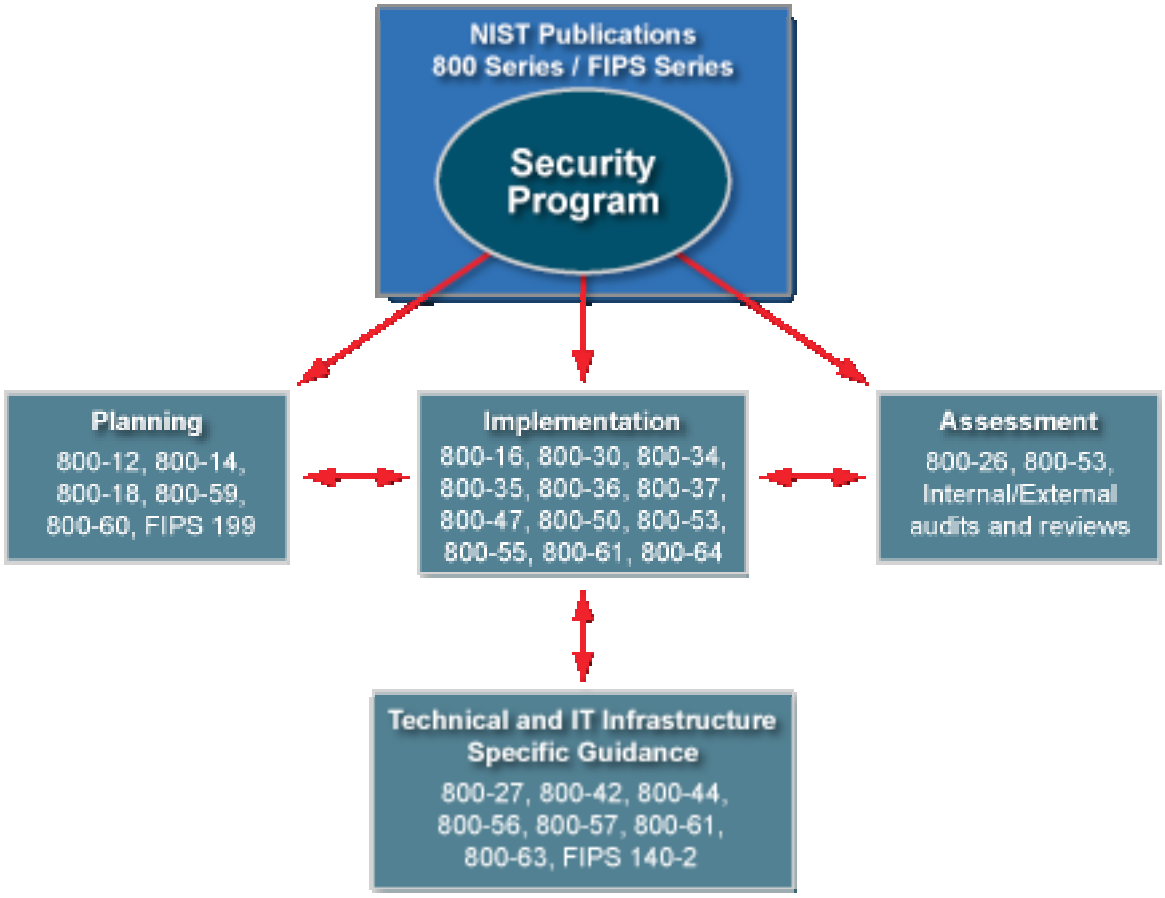

Figure 2. Key Publications for Establishing and Supporting a Security Program

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 are information security programs in place and trained personnel assigned to manage and support the programs. 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 that 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.

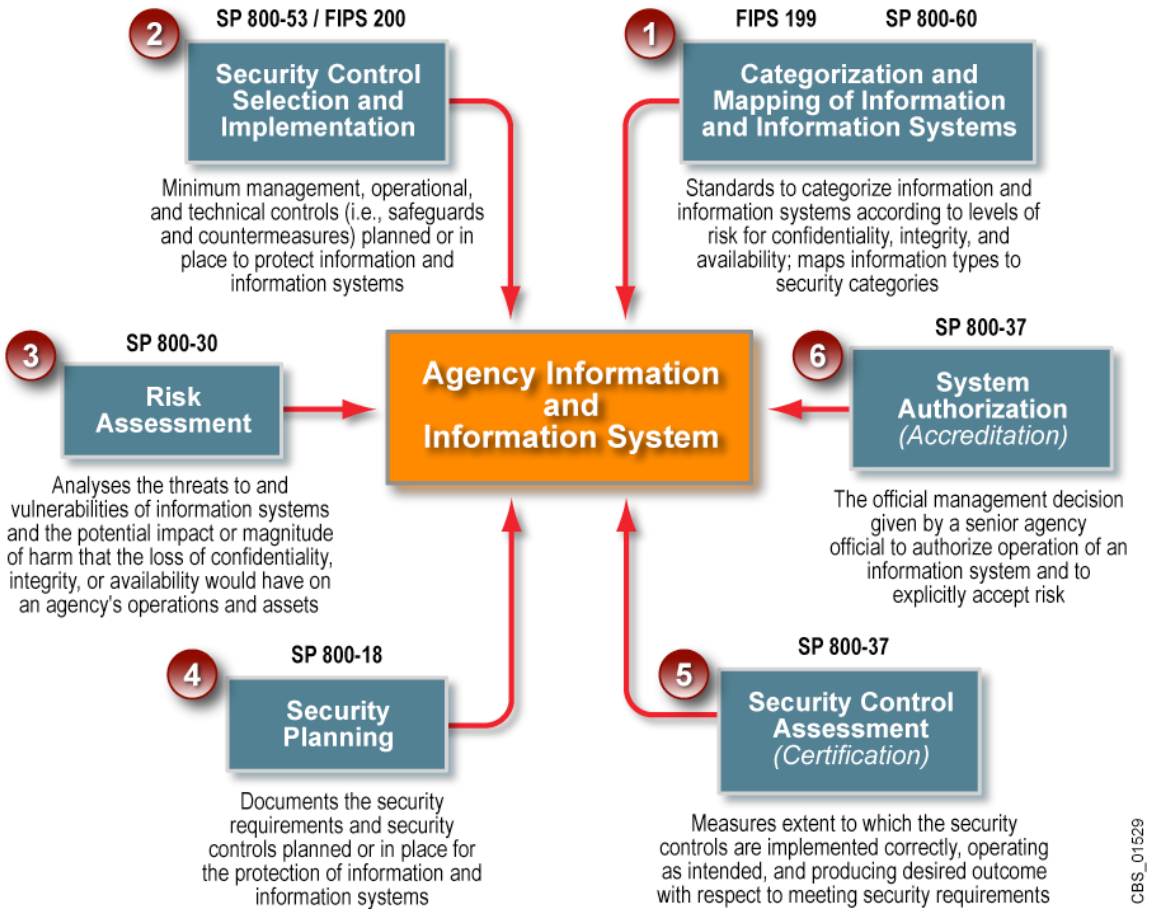

Figure 3. NIST Publications Directly Supporting Federal C&A Requirements

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, Standards for Security Categorization of Federal Information and Information Systems

- 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, Guide for Mapping Types of Information and Information Systems to Security Categories

- 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 ,Recommended Security Controls for Federal Information Systems [6]

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

SP 800-30, Risk Management Guide for Information Technology Systems

- 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, Guide for Developing Security Plans for Information Technology Systems

- Provides guidance on preparation of system security plans.

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

- Identifies key security components for both application and general support systems.

SP 800-37, Guide for Security Certification and Accreditation of Federal Information Systems

- Establishes guidelines (including tasks and subtasks) for certification and accreditation of 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 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 their functions and use of EPHI. All HIPAA covered entities, which includes some federal agencies, must comply with the Security Rule. The Security Rule specifically focuses on protecting the confidentiality, integrity, and availability of EPHI, as defined in the Security Rule. The EPHI that a covered entity creates, receives, maintains, or transmits must be protected against reasonably anticipated threats, hazards, and impermissible uses and/or disclosures. In general, the requirements, standards, and implementation specifications of the Security Rule apply to the following covered entities:

- **Covered Health Care Providers—** Any provider of medical or other health services, or supplies, who transmits any health information in electronic form in connection with a transaction for which HHS has adopted a standard.
- **Health Plans—** Any individual or group plan that provides or pays the cost of medical care (e.g., a health insurance issuer and the Medicare and Medicaid programs).
- **Health Care Clearinghouses—** A public or private entity that processes another entity's health care transactions from a standard format to a non-standard format, or vice-versa.
- **Medicare Prescription Drug Card Sponsors** – A nongovernmental entity that offers an endorsed discount drug program under the Medicare Modernization Act. This fourth category of "covered entity" will remain in effect until the drug card program ends in 2006.

This section identifies the main goals, explains some of the structure and organization, and identifies the purpose of the sections of the Security Rule.

3.1 Security Rule Goals and Objectives

As required by the "Security standards: General rules"[7] section of the HIPAA Security Rule, each covered entity must:

- Ensure the confidentiality, integrity, and availability of EPHI that it creates, receives, maintains, or transmits,
- Protect against any reasonably anticipated threats and hazards to the security or integrity of EPHI, and
- Protect against reasonably anticipated uses or disclosures of such information that are not permitted by the Privacy Rule.

In complying with this section of the Security Rule, covered entities must be aware of the definitions provided for confidentiality, integrity, and availability as given by § 164.304:

- **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 have not been altered or destroyed in an unauthorized manner."

[7] See 45 C.F.R. § 164.306(a).

- **Availability** is "the property that data or information is accessible and useable 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 standards. 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. The Security Rule is separated into six main sections that each include several standards and implementation specifications a covered entity must address.[8] Each of the six sections is listed below.

- **Security standards: General Rules** - includes the general requirements all covered entities must meet; establishes flexibility of approach; identifies standards and implementation specifications (both required and addressable); outlines decisions a covered entity must make regarding addressable implementation specifications; and requires maintenance of security measures to continue reasonable and appropriate protection of electronic protected health information.

- **Administrative Safeguards -** are defined in the Security Rule as the "administrative actions and policies, and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."

- **Physical Safeguards -** are defined as the "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."

- **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."

- **Organizational Requirements -** includes standards for business associate contracts and other arrangements, including memoranda of understanding between a covered entity and a business associate when both entities are government organizations; and requirements for group health plans.

- **Policies and Procedures and Documentation Requirements** - requires implementation of reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of the Security Rule; maintenance of written (which may be electronic) documentation and/or records that includes policies, procedures, actions, activities, or assessments required by the Security Rule; and retention, availability and update requirements related to the documentation.

Within the Security Rule sections are standards and implementation specifications. Each HIPAA Security Rule standard is required. A covered entity is required to comply with all standards of the Security Rule with respect to all EPHI.

[8] Sections of the HIPAA regulations that are included in the Security Rule and therefore addressed in this document but do not have their own modules are *Part 160 — General Administrative Requirements* § 160.103, *Definitions*; *Part 164 — Security and Privacy* §§ 164.103, *Definitions*; 164.104, *Applicability*; 164.105, *Organizational requirements* (discussed in section 4 of this document), 164.302 *Applicability*; 164.304, *Definitions*; 164.306, *Security standards: General rules* (discussed in section 3.1 of this document), and 164.318, *Compliance dates for the initial implementation of the security standards.*

Many of the standards contain implementation specifications. An implementation specification is a more detailed description of the method or approach covered entities can use to meet a particular standard.[9] Implementation specifications are either required or addressable. However, regardless of whether a standard includes implementation specifications, covered entities must comply with each standard.

- A **required** implementation specification is similar to a standard, in that a covered entity must comply with it.
- For **addressable** implementation specifications covered entities must perform an assessment to determine whether the implementation specification is a reasonable and appropriate safeguard for implementation in the covered entity's environment. In general, after performing the assessment a covered entity decides if it will implement the addressable implementation specification; implement an equivalent alternative measure that allows the entity to comply with the standard; or not implement the addressable specification or any alternative measures, if equivalent measures are not reasonable and appropriate within its environment. Covered entities are required to document these assessments and all decisions. For federal agencies, however, all of the HIPAA Security Rule's addressable implementation specifications will most likely be reasonable and appropriate safeguards for implementation, given their sizes, missions, and resources.

Where there are no implementation specifications identified in the Security Rule for a particular standard, such as for the "Assigned Security Responsibility" and "Evaluation" standards, compliance with the standard itself is required.

Anyone seeking clarification regarding the principles of the HIPAA Security Rule should send inquiries to the CMS e-mail address askhipaa@cms.hhs.gov, or contact the CMS HIPAA Hotline, 1-866-282-0659.

3.3 Safeguards Sections of the Security Rule

Table 2 lists the standards and implementation specifications within the Administrative, Physical, and Technical Safeguards sections of the Security Rule. The table is categorized according to the categorization of standards within each of the safeguards sections in the Security Rule.

- Column 1 of the table lists the Security Rule standards.
- Column 2 indicates the regulatory citation to the appropriate section of the Security Rule where the standard can be found.
- Column 3 lists the implementation specifications associated with the standard, if any exist, and designates the specification as required or addressable.

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

[9] For more information on the required analysis used to determine the manner of implementation of an implementation specification, see § 164.306(d) of the HIPAA Security Rule (Security standards — General rules: Flexibility of approach).

Table 2. HIPAA Security Rule Standards and Implementation Specifications[10]

Standards	Sections	Implementation Specifications (R)=Required (A)=Addressable	
Administrative Safeguards			
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R)	Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	[None]	
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure (A) Termination Procedures (A)	
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Functions (R) Access Authorization (A) Access Establishment and Modification (A)	
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)	
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)	
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedures (A) 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) Facility Security Plan (A) Access Control and Validation Procedures (A) 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) Media Re-use (R)	Accountability (A) Data Backup and Storage (A)
Technical Safeguards			
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R)	Automatic Logoff (A) 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)

[10] 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 also potentially relevant to the HIPAA Security Rule standards and implementation specifications listed in Table 2. In the following section, security measures relevant to these HIPAA Security Rule 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 Rule Standards

In this section, security measures from NIST publications that are relevant to each section of the Security Rule are presented. Each standard is presented in a consistent module format.

The modules are designed to make it easy to start the thought process for implementing the Security Rule. The modules provide an overview of the information available in NIST's publications. The modules are but one approach, and their use is completely optional. There may be other methods of consideration more useful to a covered entity based upon its unique operations.

The modules highlight but are not meant to be prescriptive of all the information a covered entity may wish to consider in implementing the Security Rule. The modules may not be considered all-inclusive of the information available in NIST publications.

The modules are composed of the following components:

The first element of each module is the ***Title*** of the HIPAA standard and the citation to where the standard can be located within the HIPAA Security Rule. The ***HIPAA Standard*** is then quoted directly as it appears within the HIPAA Security Rule. Compliance with each HIPAA Security Rule standard is required.

The ***Key Activities*** column suggests, for each HIPAA Security Rule standard, actions that are usually associated with the security function or functions suggested by that standard. Some of these key activities are also the implementation specifications of the HIPAA Security Rule, discussed in Section 3.2, *Security Rule Organization*, and listed in Section 3.3, Table 2. Each key activity that is also an implementation specification has been identified as such in the module (in italics in the Description section of the module), along with a note as to whether the implementation specification is required or addressable. Other key activities would normally be performed as part of one or more of the related implementation specifications under the standard, but are listed separately for clarity of presentation. Where such a relationship exists it is indicated in an accompanying footnote.

Other key activities are not implementation specifications. These activities are not specifically discussed or required by the HIPAA Security Rule, and their inclusion here is in no way meant to expand upon the intent or requirements of the Security Rule. Many of these activities, however, are usually included in a robust security process, and many will be required of federal entities under other federal laws, regulations, or procedures that may or may not be discussed within this document.

The modules address all HIPAA Security Rule standards and all associated implementation specifications, both required and addressable. Six of the standards include all the necessary instructions for implementation and have no associated implementation specifications.[11] However, as noted earlier in this document, even if there are no implementation specifications outlined in the Security Rule, such as with "Assigned Security Responsibility" and "Evaluation," compliance with the standard itself is still required.

[11] Standards that do not contain implementation specifications—that "themselves also serve as the implementation specification," as stated in the preamble to the HIPAA Security Rule—are those described in Sections 4.2 (*HIPAA Standard: Assigned Security Responsibility*); 4.8 (*HIPAA Standard: Evaluation*); 4.11 (*HIPAA Standard: Workstation Use*); 4.12 (*HIPAA Standard: Workstation Security*), 4.15 (*HIPAA Standard: Audit Controls*); and 4.17 (*HIPAA Standard: Person or Entity Authentication*).

The key activities are illustrative and not all-inclusive. There will be many additional activities an organization will need to consider, specific to its own operations that are not included in the key activities of the modules. Each entity will need to identify what activities beyond those listed in the modules are necessary and appropriate in its environment, implement those activities, and document them.

The modules are meant to serve as only a general introduction to the security topics raised by the HIPAA Security Rule. For more detailed information about the key activities, consult one or more NIST publications referenced for the subject HIPAA standard. Anyone seeking clarification regarding the principles of the HIPAA Security Rule should send inquiries to the CMS e-mail address, askhipaa@cms.hhs.gov, or contact the CMS HIPAA Hotline, 1-866-282-0659.

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 first description bullet of each key activity that is also an implementation specification includes the Security Rule implementation specification text in italics. When relationships exist between description bullets and other Security Rule standards or implementation specifications it is indicated in an accompanying footnote. The NIST publications identified as an ***Introductory Reference*** for the HIPAA Security Rule standard can be consulted for more detailed information about the security topic.

The third column, ***Sample Questions***, includes some questions to determine whether or not the elements described have actually been considered or completed. These sample questions are not exhaustive but merely indicative of relevant questions that could be asked. 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 standards. 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. Note, however, that negative answers to these questions should prompt the covered entity to consider whether it needs to take further action in order to comply with the standards. In fact, it is expected that many organizations with existing information security infrastructure already in place will have considered most of the Sample Questions. The questions an organization asks in assessing and developing its security program should be tailored to fit the unique circumstances of each entity.

The bottom row of most modules includes additional NIST documents that may be consulted as ***Primary References*** and ***Supplemental References*** for implementing the standards and implementation specifications of the HIPAA Security Rule. These publications are also referenced in the HIPAA Security Rule/ NIST Publications Crosswalk table in Appendix D.

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. The examples suggest actions and issues that could arise, but are not comprehensive descriptions of the actions an organization must perform to address the HIPAA Security Rule standard. The actual activities necessary to implement the standard requirement for any given entity may vary substantially depending on organization mission, size, and scope. There may be mitigating factors an entity should consider that are beyond the context of the examples provided. The examples are for illustrative purposes only and are not meant to imply any degree of HIPAA compliance.

The examples describe the efforts of two hypothetical federal agencies that are also HIPAA covered entities. An overview of the environmental and information systems characteristics of each covered entity is provided below. The examples describe how each of the covered entities has chosen to address certain

standards and implementation specifications of the HIPAA Security Rule. Again, the examples are provided for informational purposes only, and appropriate and necessary activities will differ for each covered entity.

Each example is followed by an ***Explanation*** that illustrates how the standard (and its implementation specifications, if any) were addressed by the hypothetical entities in the previous example. Each explanation contains references and citations to the HIPAA Security Rule.

Overview of Example Health Plan:

Example Health Plan (EXHP) is a large federal health plan with operations in multiple states. The overall structure of the organization includes a main office and remote state offices in each state the health plan serves. The main office is responsible for establishing security policy, standards and technology for the entire covered entity. The remote state offices are responsible for implementation of the policy, standards and technology within their local environment. EXHP has a single standardized information system that processes, stores and transmits EPHI. The system was implemented five years ago. The information system is distributed among the offices, with the primary data center in the main office.

Overview of Example Hybrid Covered Entity and Large Healthcare Provider:

Example Hybrid Covered Entity (EXHCE) is a government organization that is also a hybrid entity. The organization has designated the healthcare provider functions of the larger organization as the health care component of the organization, pursuant to § 164.105 of the HIPAA Security Rule. The healthcare provider functions are not the primary functions of the organization. The information systems that store electronic protected health information (EPHI) for the health care component are kept separate from the primary non-covered functions.

Example Large Healthcare Provider (EXLHCP) is the health care component (the part of the hybrid entity that performs the functions that make the hybrid entity a covered entity) under EXHCE and is a large federal healthcare delivery network with over 50 hospitals in multiple states. The structure of EXLHCP includes a central management organization and individual management teams responsible for single or multiple hospital locations. The central management organization is responsible for establishing security policy, standards and technology for the entire organization. Each of the hospital management teams is responsible for implementing the policy, standards and technology within their local environments.

EXLHCP has developed a standard list of technologies for use within the organization. Central management allows each of the local hospitals to implement the technology that best meets their individual needs. The list of technologies includes over 30 different information systems, used by the local hospitals that contain EPHI. Some of the systems were implemented over 10 years ago. Other systems have been, or have begun to be implemented, within the last 12 months. Some hospitals have implemented an information system from the same vendor but are operating on different versions.

Overview of Organizational Requirements:

Section 164.105 of the HIPAA Security Rule, *Organizational Requirements*, sets out the special requirements that covered entities must meet if they qualify to be able to designate themselves as "hybrid entities" or "affiliated covered entities" if they choose to do so. This document will not discuss these

organizational requirements in detail, as they do not set out general security principles. HIPAA covered entities are encouraged to review this section of the HIPAA Security Rule in full and seek further guidance. Section 164.105 contains three standards:

- Section 164.105(a)(1), *Standard: Health Care Component,* sets out special requirements for health care components of hybrid entities. Among other effects, this section establishes which provisions of the HIPAA Security Rule apply only to the health care component and which apply to the entire hybrid entity; requires the health care component to protect EPHI from being impermissibly disclosed to other components of the hybrid entity; and establishes requirements for designating components of a hybrid entity as health care components.

- Section 164.105(b)(1), *Standard: Affiliated Covered Entities*, among other effects, establishes that affiliated covered entities must safeguard EPHI consistently with the administrative, technical and physical standards of the HIPAA Security Rule.

- Section 164.105(c)(1), *Standard: Documentation* states that covered entities must retain documentation of the covered entity's designation as a hybrid entity or affiliated covered entity and retain that documentation for 6 years from the date of its creation or the date it was last in effect, whichever is greater.

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 EPHI. • Include all hardware and software that are used to collect, store, process, or transmit EPHI. • Analyze business functions and verify ownership and control of information system elements as necessary.	• Are all hardware and software for which the organization is responsible periodically inventoried? • Have hardware and software that maintains or transmits EPHI been identified? • Is the current information system configuration documented, including connections to other systems? • 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[12] **Implementation Specification (Required)**	• *Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by the covered entity.* Risk assessments typically include the following steps: • Determine system characterization: – Hardware – Software – System interfaces – Data and information – People	• Are there any prior risk assessments, audit comments, security requirements, and/or security test results? • Is there intelligence available from agencies, the Office of the Inspector General (OIG), the US-CERT, virus alerts, and/or vendors? • What are the current and planned controls? • Is the facility located in a region prone to any natural

[12] The risks that must be assessed are the risks of noncompliance with the requirements of § 164.306(a) (General Rules) of the HIPAA Security Rule: (1) ensure the confidentiality, integrity, and availability of all EPHI the covered entity creates, receives, maintains or transmits, (2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information, (3) protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part, and (4) ensure compliance with this subpart by its workforce..

[13] See Section 4.22, *HIPAA Standard: Documentation*

Key Activities	Description	Sample Questions
	– System mission. • Identify any vulnerability or weaknesses in security procedures or safeguards. • Identify events that can negatively impact security. • Identify current controls in place • Identify the potential impact that a security breach could have on an organization's operations or assets, including loss of integrity, availability, or confidentiality. • Recommend security controls for the information and the system, including all the technical and non-technical protections in place to address security concerns. • Determine residual risk. • Document all outputs and outcomes from the risk assessment activities.[13]	disasters, such as earthquakes, floods, or fires? • Has responsibility been assigned to check all hardware and software to determine whether selected security settings are enabled? • Is there an analysis of current safeguards and their effectiveness relative to the identified risks? • Have all processes involving EPHI been considered, including creating, receiving, maintaining, and transmitting it?
3. Implement a Risk Management Program[14] **Implementation Specification (Required)**	• *Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).*	• Do current safeguards ensure the confidentiality, integrity, and availability of all EPHI? • Do current safeguards protect against reasonably anticipated uses or disclosures of EPHI that are not permitted by the Privacy Rule? • Has the covered entity protected against all reasonably anticipated threats or hazards to the security and integrity of EPHI? • Has the covered entity assured compliance with all policies and procedures by its workforce?
4. Acquire IT Systems and Services[15, 16]	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: • Applicability of the IT solution to the intended environment. • The sensitivity of the data. • The organization's security policies, procedures, and standards. • Other requirements such as resources available for operation, maintenance, and training.	• How well will new security controls work with the existing IT architecture? • Have the security requirements of the organization been compared with the security features of existing or proposed hardware and software? • Has a cost- benefit analysis been conducted to determine the reasonableness of the investment given the security risks identified? • Has a training strategy

[14] See Section 164.306 of the HIPAA Security Rule.

Key Activities	Description	Sample Questions
		been developed?[17]
5. Create and Deploy Policies and Procedures[18, 19]	Implement the decisions concerning the management, operational, and technical controls selected to mitigate identified risks. • Create policies that clearly establish roles and responsibilities and assign ultimate responsibility for the implementation of each control to particular individuals or offices.[20] • Create procedures to be followed to accomplish particular security related tasks.	• Are policies and procedures in place for security? • Is there a formal (documented) system security plan? • Is there a formal contingency plan?[21] • Is there a process for communicating policies and procedures to the affected employees? • Are policies and procedures reviewed and updated as needed?
6. Develop and Implement a Sanction Policy[22] **Implementation Specification (Required)**	• *Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.* • Develop policies and procedures for imposing appropriate sanctions (e.g., reprimand, termination) for noncompliance with the organization's security policies. • Implement sanction policy as cases arise.	• Is there a formal process in place to address system misuse, abuse, and fraudulent activity? • Have employees been made aware of policies concerning sanctions for inappropriate access, use and disclosure of EPHI? • Has the need and appropriateness of a tiered structure of sanctions that accounts for the magnitude of harm and possible types of inappropriate disclosures been considered? • How will managers and employees be notified regarding suspect activity?
7. Develop and Deploy the Information System Activity Review Process **Implementation Specification (Required)**	• *Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.*	• Who is responsible for the overall process and results?[23] • How often will reviews take place? • How often will review results be analyzed? • What is the organization's sanction policy for employee violations? • Where will audit information reside (e.g., separate server)?

[15] See Section 164.306(b) of the HIPAA Security Rule.
[16] See Key Activity 4.1.3, *Implement a Risk Management Program.* This activity and all associated bullets in the Description and Sample Questions are part of the process of addressing the risk management implementation specification.
[17] See Section 4.5, *HIPAA Standard: Security Awareness and Training*.
[18] See Section 4.21, *HIPAA Standard: Policies and Procedures.*
[19] See Key Activity 4.1.3, *Implement a Risk Management Program.* This activity and all associated bullets in the Description and Sample Questions are part of the process of addressing the risk management implementation specification.
[20] See Section 4.21, *HIPAA Standard: Policies and Procedures* and Section 4.22, *HIPAA Standard: Documentation.*
[21] See Section 4.7, *HIPAA Standard: Contingency Plan.*
[22] See Section 164.306 of the HIPAA Security Rule.
[23] See Section 4.2, *HIPAA Standard: Assigned Security Responsibility*.

Key Activities	Description	Sample Questions
8. Develop Appropriate Standard Operating Procedures[24]	• 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? • Where will monitoring reports be filed and maintained?
9. Implement the Information System Activity Review and Audit Process[25]	• Activate the necessary review process. • Begin auditing and logging activity.	• What mechanisms will be implemented to assess the effectiveness of the review process (metrics)? • What is the plan to revise the review process when needed?
Supplemental References	• NIST SP 800-14 • NIST SP 800-18 • NIST SP 800-26 • NIST SP 800-27 • NIST SP 800-30 • NIST SP 800-37 • NIST SP 800-53 • NIST SP 800-60 • FIPS 199	

Example:

Example Health Plan (EXHP) established a formal security management program several years ago to protect the confidentiality, integrity and availability of all electronic information. Initially, the security management program was implemented to address other Federal laws and requirements (e.g., HIPAA Privacy Rule and Federal Information Security Management Act (FISMA)). To comply with the HIPAA Security Rule, the covered entity has specifically included EPHI as a subset of the electronic information it protects (§ 164.306(a)). These examples address how EXHP will comply with the HIPAA Security Rule.

The security management program includes formal security risk analysis and risk management processes. The main office and all remote state offices have been performing this formal process since 1996. The main office developed a formal risk analysis tool and released it to the remote state offices. All entities implement the tool independently using internal resources with information security expertise. The tool captures threat and vulnerability information relevant to each location. The risk analysis tool generates reports that include qualified and quantified risks. In addition to the risk analysis tool, the main office developed risk management guidelines to focus the security measures implemented for certain types of risks. The remote state offices use the risk management guidelines in their decision making process. The covered entity has determined this process meets the intent of the Security Rule and it will be continued (§§ 164.308(a)(1)(ii)(A) – (B)).

After performing risk analyses for many years, the main office has identified several instances of internal employees creating organizational risk (e.g., sharing passwords or not logging off workstations). Therefore, the main office developed a more stringent sanction policy for violations of the organization's

[24] See Key Activity 4.1.7, *Develop and Deploy the Information System Activity Review Process*. This activity and all associated bullets in the Description and Sample Questions are part of the process of addressing the information system activity review implementation specification.
[25] See Key Activity 4.1.7, *Develop and Deploy the Information System Activity Review Process*. This activity and all associated bullets in the Description and Sample Questions are part of the process of addressing the information system activity review implementation specification.

policies and procedures related to electronic information. The policy is distributed to all remote offices and implemented without revision. The main office determined it was necessary to implement this policy without modification to ensure consistent application of identified sanctions (§ 164.308(a)(1)(ii)(C)).

Another significant factor in EXHP's security management program is the ability to review activities performed in the primary information system. The main office requires the information system to have minimum security capabilities. (These minimum capabilities are described in the Technical Safeguards examples.) The main office requires information systems to have the capability to generate reports related to the review of those general security safeguards. Manually generated security incident reports are also reviewed. The main office requires review of these information system activity reports at least twice a week or more frequently as needed. Any reviews that identify significant issues are handled through the security incident response process described later in Section 4.6 of this document (§ 164.308(a)(1)(ii)(D)).

Explanation:

The covered entity's decision to maintain the current security management program, which includes the risk analysis and risk management processes, is appropriate for its environment, if it addresses the standards and implementation specifications at §§ 164.306(a), and 164.308(a)(1)(ii)(A) and (B). The implementation specifications at §§ 164.308(a)(1)(ii)(A) and (B) require an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI and the implementation of security measures to reduce risks and vulnerabilities identified during the risk analysis to a reasonable and appropriate level. If the risk analysis and management process do not sufficiently identify and reduce risks to and vulnerabilities of EPHI, then the processes must be revised.

The decision to develop a more stringent sanction policy and procedures is a permissible way of meeting the requirements of the standard at § 164.306(a)(4) and the implementation specification at § 164.308(a)(1)(ii)(C). 45 CFR § 164.306(a)(4) requires a covered entity to ensure compliance with the Security Rule by all workforce members. The implementation specification at § 164.308(a)(1)(ii)(C) requires a covered entity to apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. If the sanction policy and procedure language does not provide those responsible for applying sanctions with a consistent means for ensuring workforce compliance with the Security Rule, then the sanction language must be revised.

The covered entity's decision to coordinate the information system activity review procedure with the technical measures available in information systems and to require the reviews to be performed weekly is reasonable and appropriate. The entity's decision meets the intent of the standard at § 164.306(a)(2) and the implementation specification at § 164.308(a)(1)(ii)(D). 45 CFR § 164.306(a)(2) requires a covered entity to protect against any reasonably anticipated threats or hazards to the security or integrity of EPHI. The implementation specification at § 164.308(a)(1)(ii)(D) requires a covered entity to implement a procedure to regularly review records of information system activity. If the logs and/or reports contain too much information to review twice a week, then the review must be performed more regularly. If the capability to generate logs and/or reports, using either technical or manual capabilities, does not support reviews twice a week, then the procedure must be revised.

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 by this subpart for the entity.*

Key Activities	Description	Sample Questions
Note: This HIPAA Standard does not include any implementation specifications.	**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 has final responsibility for security. • 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— • Oversees the development and communication of security policies and procedures? • Is responsible for conducting the risk assessment? • Handles the results of periodic security evaluations? • Directs IT security purchasing and investment? • Ensures that security concerns have been addressed in system implementation?
2. Assign and Document the Individual's Responsibility	• Document the assignment to one individual's responsibilities in a job description.[26] • Communicate this assigned role to the entire organization.	• Is there a complete job description that accurately reflects assigned security duties and responsibilities? • Have the staff members in the organization been notified as to whom to call in the event of a security problem?[27]
Supplemental References	• NIST SP 800-14 • NIST SP 800-26 • NIST SP 800-53	

Example:

Example Large Healthcare Provider (EXLHCP) has used an Information Security Committee consisting of members from the central management organization and individuals from the hospital locations. The responsibilities of the committee include development of security policy, review of security incidents, discussions of security technology, and other discussions of relevant security topics. This structure has worked well for the organization for years. Therefore, the covered entity made the decision to assign the chairman of this committee, the Chief Security Officer at the central management organization, as the overall security official as required by § 164.308(a)(2). The security official's expanded responsibilities include oversight and accountability for all information security activities of EXLHCP. The functions of the committee remain the same.

[26] See Standard 4.22, *Standard: Documentation*.
[27] See Standard 4.5, *Security Awareness and Training*, and 4.6, *Security Incident Procedures.*

To maintain consistent implementation of the organization's security program, the security official and Information Security Committee decided to require each hospital location to appoint a local security official. Most local hospitals elected to appoint their Information Security Committee representative as their security official, as well. At other hospitals, a new security official with dedicated responsibility for the local security program was appointed. The local security officials report to the central security official. The responsibility of the local security officials is to implement the organization's security program at their respective hospitals.

Explanation:

The covered entity's decision to assign security responsibility while maintaining the existing committee structure is reasonable and appropriate. The assigned security responsibility standard (§ 164.308(a)(2)) requires a covered entity to identify a security official to be responsible for development and implementation of required security policies and procedures. The organization identified one individual as the security official with responsibility for the entire information security program. That individual's duties include being chairman of the committee, responsibility for development of policy and procedures, control of information security budgeting, oversight of local security officials, and other relevant duties. The Security Rule does not prohibit a covered entity from maintaining an information security committee or similar structure to assist the security official in making organizational decisions, as long as the security official has ultimate responsibility. If the security official's responsibilities do not meet the requirements of § 164.308(a)(2), then the assignment must be changed. The Security Rule also does not prohibit the assignment of additional security officials in large organizations with multiple locations as long as one individual has been assigned ultimate responsibility.

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. Implement Procedures for Authorization and/or Supervision **Implementation Specification (Addressable)**	• *Implement procedures for the authorization and/or supervision of workforce members who work with EPHI or in locations where it might be accessed.*	• Have chains of command and lines of authority been established? • Have staff members been made aware of the identity and roles of their supervisors?
2. Establish Clear Job Descriptions and Responsibilities[28]	• Define roles and responsibilities for all job functions. • Assign appropriate levels of security oversight, training, and access. • Identify in writing who has the business need—and who has been granted permission—to view, alter, retrieve, and store EPHI, and at what times, under what circumstances, and for what purposes.[29]	• Are there written job descriptions that are correlated with appropriate levels of access?
3. Establish Criteria and Procedures for Hiring and Assigning Tasks[30]	• 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. • Ensure that these requirements are included as part of the personnel hiring process.	• Are the qualifications of candidates for specific positions been checked against the job description? • Have determinations been made that candidates for specific positions are able to perform the tasks of those positions?
4. Establish a Workforce Clearance Procedure **Implementation Specification (Addressable)**	• *Implement procedures to determine that the access of a workforce member to EPHI is appropriate.* • Implement appropriate screening of persons who will have access to EPHI. • Implement a procedure for obtaining clearance from appropriate offices or individuals	• Is there an implementation strategy that supports the designated access authorities? • Are applicants' employment and educational references checked, if reasonable and appropriate? • Have background checks been completed, if reasonable and appropriate?

[28] See Key Activity 4.3.1, *Implement Procedures for Authorization and/or Supervision.* This activity and all associated bullets in the Description and Sample Questions are part of the procedures for authorization and/or supervision.
[29] See Section 4.22, *HIPAA Standard: Documentation.*
[30] See Key Activity 4.3.1, *Implement Procedures for Authorization and/or Supervision.* This activity and all associated bullets in the Description and Sample Questions are part of the procedures for authorization and/or supervision.

Key Activities	Description	Sample Questions
	where access is provided or terminated.	• Do procedures exist for obtaining appropriate sign-offs to grant or terminate access to EPHI?
5. Establish Termination Procedures **Implementation Specification (Addressable)**	• *Implement procedures for terminating access to EPHI when the employment of a workforce member ends or as required by determinations made as specified in §164.308(a)(3)(ii)(B).* • 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. • 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), if reasonable and appropriate? • 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, and delivery of any needed data solely under the employee's control)?
Supplemental References	• NIST SP 800-14 • NIST SP 800-26 • NIST SP 800-53	

Example:

The EXHP has a standardized primary information system and is able to establish clear policies and procedures for the authorization, clearance, establishment, modification and termination of a workforce member's access to the system and locations where EPHI is accessible (§§ 164.308(a)(3) & (4)). A large organizational project was started two years ago to streamline and automate this entire process for all locations. EXHP expects the updated processes to improve departmental coordination, save resource costs, reduce certain vulnerabilities in the current process, and ensure compliance with the Security Rule.

An Intranet based system is being implemented to automate the existing access procedures. The updated procedures will still involve cooperation between the main office and remote offices but the automated system will reduce time lags in the process. During their risk analysis, the covered entity determined that delays in authorizing and establishing access could create workforce productivity losses. The risk analysis also identified that delays in notification for modification or termination of access create undue risk of unauthorized access (§ 164.308(a)(1)(ii)(A)).

The Intranet system contains a list of all established workforce job classifications and the pre-authorized information access levels based on the job classification. The job classification list and pre-authorized access levels were reviewed and approved by all relevant department managers and supervisors at the main office and remote locations (§ 164.308(a)(3)(ii)(A)). The job classifications are consistent across entities.

The workforce job classifications and pre-authorized access levels in the system are directly related to approved functions each employee is responsible for performing. The job classifications were previously developed to address other federal law and organizational needs (§ 164.308(a)(4)). Once the appropriate authorizations are granted, the workforce member can automatically be set up, or established, with appropriate access levels to the relevant information systems needed for their specific job.

Current manual procedures requiring a workforce member's supervisor to manually sign-off, or clear, that access is appropriate, and will be performed using the electronic system. The Human Resources (HR) department enters the workforce member's employment, educational, and/or background check information (as required) into the system. Once this is complete, the hiring manager receives a notification via email to log-in to the system and sign-off on members' access. (§ 164.308(a)(3)(ii)(B))

After the department manager signs off, the Information Systems (IS) department, at the relevant location, receives an email notification to establish access for the workforce member. The notification includes the type of access needed to perform that individual's job functions. (§ 164.308(a)(4)(ii)(B)) The information system records the access levels provided to the workforce member and can report the information as needed. (§ 164.308(a)(4)(ii)(C))

The Intranet system also contains information on the termination and job modification processes. When an employee is terminated or changes job classifications, the department manager or HR initiates the termination or modification process. Once the process is initiated, notifications are sent to the appropriate HR and IS personnel. The termination or modification notification includes relevant details for all parties involved to perform their respective termination or modification of access processes. For terminations, the HR department collects all devices that provide physical access. Finally, the IS department removes or modifies all information system access. (§ 164.308(a)(3)(ii)(C))

Every six months a report of all workforce members and associated access levels is generated by the IS department and sent to the relevant department managers for review. The department managers are responsible for reviewing the list for accuracy and notifying IS, through the Intranet system, if a workforce member's access should be modified or terminated. This final check is used to verify accuracy of access levels and the overall success of the new Intranet system.

The covered entity reviewed business operations to identify health care clearinghouse functions as required by the implementation specification at § 164.308(a)(4)(ii)(A). The review verified health care clearinghouse functions are not performed. The findings are documented.

Explanation:

The covered entity's decision to address the standards for Workforce Security (§164.308(a)(3)) and Information Access Management (§ 164.308(a)(4)) as an integrated process is permissible based on the facts provided. 45 CFR § 164.308(a)(3) references § 164.308(a)(4), which appears to complete the process for providing workforce members access to EPHI.

The decision to use existing policies and procedures as the basis for development and implementation of the automated Intranet based access system is appropriate based on the facts presented, if the policies and procedures address the requirements of §§ 164.306(a)(3), 164.308(a)(3) and 164.308(a)(4). 45 CFR § 164.306(a)(3) requires covered entities to protect against any reasonably anticipated uses or disclosures of EPHI that are not permitted by the HIPAA Privacy Rule. The standard and implementation specifications of § 164.308(a)(3) require a covered entity to implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI, as provided under paragraph (a)(4) [Information Access Management], and to prevent those workforce members who do not have access authorization under paragraph (a)(4) [Information Access Management] from obtaining access to EPHI. 45 CFR § 164.308(a)(4) requires covered entities to implement policies and procedures for authorizing access to EPHI that are consistent with the applicable requirements of the Privacy Rule. The covered entity would still be able to achieve compliance using the automated Intranet access system if the existing policies and procedures for the authorization, clearance, establishment, modification and termination of

workforce member's access to the information system and locations where EPHI is accessible address the requirements of the standards identified above and are incorporated into the Intranet access system.

This example assumes the Human Resources (HR) department is performing a manual process to verify the workforce member's background and job qualifications before entering the employment information into the system. If the HR department is not performing some method of workforce clearance procedure before initiating the access authorization process, then the process must be updated to include this activity. (§ 164.308(a)(3)(ii)(B))

The covered entity's decision to continue to require sign-off by a workforce member's supervisor for access to EPHI but automate the process is appropriate for this entity, if the automated process provides a means of verifying the supervisor's sign-off. If the sign-off cannot be verified during the automated or subsequent manual process, then a mechanism for verification must be developed and added to the process (§ 164.308(a)(3)(ii)(A)).

The example states the covered entity is using a decentralized method of establishing, modifying and terminating user access. The IS department at each location is responsible for managing user access within the information system. The Security Rule does not require a specific method (e.g., decentralized or centralized) for performing access functions within information systems, as long as the covered entity has a method in place. The entity's decision to use a decentralized method for establishing, modifying and terminating user access is appropriate for its environment, if the procedures are implemented at all locations (§ 164.308(a)(4)(ii)(B)).

The covered entity's decision to automate the termination and job modification process within the Intranet system is appropriate given the covered entity's circumstances, if the notifications generated by the system allow the assigned departments to perform their required termination or modification functions in a timely manner. The entity's risk analysis uncovered time delays in the termination process during the exchange of termination information from the department managers to the HR department and finally to the IS departments. The time delays, upwards of 60 days, allowed a workforce member who was no longer employed by the entity to access information systems with EPHI. If the automated Intranet system does not reduce the information sharing time delays to reasonable levels, the system must be modified to ensure only authorized workforce members can access EPHI using a workstation, transaction, program, process or other mechanism (§ 164.308(a)(4)(ii)(C)).

The covered entity's finding and documentation that it does not engage in clearinghouse functions is an appropriate means of documenting that §164.308(a)(4)(ii)(A) does not apply.

4.4 Information Access Management (§ 164.308(a)(4))[31]

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. Isolate Healthcare Clearinghouse Functions[32] **Implementation Specification (Required)**	• *If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the EPHI of the clearinghouse from unauthorized access by the larger organization.* • Determine if a component of the covered entity constitutes a health care clearinghouse under the HIPAA Security Rule. • If no clearinghouse functions exists, document this finding. • If a clearinghouse exists within the organization, implement procedures for access consistent with the HIPAA Privacy Rule.	• Does the health care clearinghouse share hardware or software with a larger organization of which it is a part? • Does the healthcare clearinghouse share staff or physical space with staff from a larger organization? • Has a separate network or subsystem been established for the healthcare clearinghouse, if reasonable and appropriate? • Has staff of the healthcare clearinghouse been trained to safeguard EPHI from disclosure to the larger organization, if required for compliance with the HIPAA Privacy Rule?
2. Implement Policies and Procedures for Authorizing Access **Implementation Specification (Addressable)**	• *Implement policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, process, or other mechanism.* • Decide how access will be granted to workforce members within the organization. • Select the basis for restricting access. • Choose between identity- based access (by name) or role-based access (by job) or other reasonable and appropriate means of access. • Determine if direct access to EPHI will ever be appropriate for individuals external to the organization (e.g., business partners or patients seeking access to their own EPHI).	• Does the organization's IT systems have the capacity to set access controls?[33] • Are there documented job descriptions that accurately reflect assigned duties and responsibilities and enforce segregation of duties?[34] • Will access be identity-based, role-based, location-based, or some combination thereof?
3. Implement Policies and Procedures for Access	• *Implement policies and procedures that, based upon the entity's access authorization policies, establish,*	• Are duties separated such that only the minimum necessary EPHI is made

[31] Note: See also Section 4.10, *HIPAA Standard: Facility Access Controls* and Section 4.14, *HIPAA Standard: Access Controls.*.
[32] Note: Where the healthcare clearinghouse is a separate legal entity, it is subject to the Security Rule whether or not the larger organization is a covered entity.
[33] See Section 4.14, *HIPAA Standard: Access Controls.*
[34] See Section 4.3, *HIPAA Standard: Workforce Security.*

Key Activities	Description	Sample Questions
Establishment and Modification **Implementation Specification (Addressable)**	*document, review, and modify a user's right of access to a workstation, transaction, program, or process.* • Establish standards for granting access. • Provide formal authorization from the appropriate authority before granting access to sensitive information.	available to each staff member based on their job requirements?
4. Evaluate Existing Security Measures Related to Access Controls[35]	• Evaluate the security features of access controls already in place, or those of any planned for implementation, as appropriate. • Determine if these security features involve alignment 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 there policies and procedures related to the security of access controls?[36] • If so, are they updated regularly? • Are authentication mechanisms used to verify the identity of those accessing systems protected from inappropriate manipulation?[37] • Does management regularly review the list of access authorizations to verify that they have not been inappropriately altered or have not been updated as necessary? [38]
Supplemental References	• NIST SP 800-14 • NIST SP 800-18 • NIST SP 800-53 • NIST SP 800-63	

Example:

NOTE: The Example and Explanation in Section 4.3, *HIPAA Standard: Workforce Security* includes content covered in this module.

[35] See Key Activity 4.4.3, *Implement Policies and Procedures for Access Establishment and Modification.* This activity and all associated bullets in the Description and Sample Questions are part of the access establishment and modification implementation specification.
[36] See Section 4.22, *HIPAA Section: Documentation.*
[37] See Section 4.17, *HIPAA Standard: Person or Entity Authentication.*
[38] See Section 4.3, *HIPAA Standard: Workforce Security.*

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

HIPAA Standard: *Implement a 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. • Interview and involve key personnel in assessing security training needs.	• What awareness, training, and education programs are needed (e.g., what is required)? • What is the current status regarding how these needs are being addressed (e.g., how well are current efforts working)? • Where are the gaps between the needs and what is being done (e.g., what more needs to be done)? • What are the training priorities?
2. Develop and Approve a Training Strategy and a Plan	• Address the specific HIPAA policies that require security awareness and training in the security awareness and training program. • Outline in the security awareness and training program 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? • What type of security training is needed to address specific technical topics based on job responsibility? • When should training be scheduled to ensure that compliance deadlines are met?
3. Protection from Malicious Software; Log-in Monitoring; and Password Management **Implementation Specifications (All Addressable)**	• As reasonable and appropriate, train employees regarding procedures for: – *Guarding against, detecting, and reporting malicious software.* – *Monitoring log-in attempts and reporting discrepancies.* – *Creating changing, and safeguarding passwords.* • Incorporate information concerning staff members' roles and responsibilities in implementing these implementation specifications into training and awareness efforts.	• Do employees know the importance of timely application of system patches to protect against malicious software and exploitation of vulnerabilities? • Are employees aware that log-in attempts may be monitored? • Do employees that monitor log-in attempts know to whom to report discrepancies? • Do employees understand their roles and responsibilities, if any, in selecting a password of appropriate strength, changing the password periodically (if required), and safeguarding their password?
4. Develop Appropriate Awareness and Training Content, Materials, and	• Select topics that may need to be included in the training materials. • Incorporate new information from e-mail advisories, online IT security daily	• Have employees received a copy of or do they have ready access to the security procedures and policies?[39]

[39] See Section 4.22, *HIPAA Standard: Documentation.*

Key Activities	Description	Sample Questions
Methods	news Web sites, and periodicals, as is reasonable and appropriate. • 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.	• Do employees know whom to contact and how to handle a security incident?[40] • Do employees understand the consequences of noncompliance with the stated security policy?[41] • Do employees who travel know how to handle physical laptop security issues and information security issues?[42] • Has the covered entity researched available training resources? • Are dedicated training staff available for delivery of security training? If not, who will deliver the training? • What is the security training budget?
5. Implement the Training	• Schedule and conduct the training outlined in the strategy and plan. • 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?
6. Implement Security Reminders **Implementation Specification (Addressable)**	• *Implement periodic security updates.* • Provide periodic security updates to staff, business associates, and contractors.	• What methods are available or already in use to make or keep employees aware of security, e.g., posters or booklets? • Is security refresher training performed on a periodic basis (e.g., annually)? • Is security awareness discussed with all new hires? • Are security topics reinforced during routine staff meetings?
7. Monitor and Evaluate Training Plan [43]	• Keep the security awareness and training program current. • Conduct training whenever changes occur in the technology and practices as appropriate. • Monitor the training program implementation to ensure all employees participate. • Implement corrective actions when problems arise.[44]	• Are employee training and professional development programs documented and monitored, if reasonable and appropriate? • How are new employees trained on security?
Primary Reference	• NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*	

[40] See Section 4.6, *HIPAA Standard: Security Incident Procedures.*
[41] See Section 4.1, *HIPAA Standard: Security Management Process.*
[42] See Section 4.13, *HIPAA Standard: Device and Media Controls.*
[43] Also required under the HIPAA Security Rule § 164.306, General Requirements, Subsection (e), *Maintenance*. See also Section 4.8, *HIPAA Standard: Evaluation.*
[44] See Section 4.1, *HIPAA Standard: Security Management Process.*

Key Activities	Description	Sample Questions
Supplemental References	• NIST SP 800-14 • NIST SP 800-16 • NIST SP 800-53	

Example:

EXLHCP has an existing mandatory confidentiality and security awareness and training program ("training program") that is provided to all workforce members including management at all locations. The covered entity determined that minimal updates are needed to meet Security Rule compliance. The current training program is delivered by a trainer during the orientation program and is refreshed annually as part of the performance evaluation process. The content covers confidentiality, privacy and security issues relevant to the organization. (§ 164.308(a)(5)(i)) The security training section was updated to reflect the topics suggested in the Security Rule, including EPHI, protection from malicious software, log-in monitoring and password management (§§ 164.308(a)(5)(ii)(B) – (D)).

The awareness program promotes key concepts of the confidentiality, privacy and security training using various methods. A monthly article discussing current hot topics is published in the employee newsletter. Each hospital location provides workforce members with security trinkets highlighting important phrases and concepts. As needed, e-mails are distributed to warn workforce members of malicious code, viruses and other urgent information security issues. (§ 164.308(a)(5)(ii)(A))

Explanation:

Under the facts set out in the example, the covered entity's decision to update the existing training program to include topics required by the Security Rule is reasonable and appropriate if the existing training program allows the entity to address the standards at §§ 164.306(a)(4) and 164.308(a)(5). 45 CFR §164.306(a)(4) requires a covered entity to ensure compliance with the Security Rule by all workforce members. The standard at § 164.308(a)(5) requires covered entities to implement a security awareness and training program from all members of its workforce (including management).

The entity's decision to use the existing training program is appropriate for its environment, if all members of the workforce, including management, receive security training. If the training program is not delivered to all workforce members, then the training program must be revised to do so.

The covered entity's decision to update the content of the security training to include addressable implementation specifications of this standard (protection from malicious software, log-in monitoring and password management) is reasonable and appropriate for its environment. In general, § 164.306(d)(3) requires covered entities to assess whether each addressable implementation specification is a reasonable and appropriate safeguard to implement in its environment. If the covered entity determines the safeguard is reasonable and appropriate the safeguard must be implemented (§§ 164.308(a)(5)(ii)(B) – (D)).

The covered entity's decision to promote security awareness among the workforce by distributing monthly articles, security trinkets and e-mail notifications is a permissible way of meeting the requirements of this implementation specification. The addressable implementation specification at § 164.308(a)(5)(ii)(A) for security reminders only requires periodic security updates. The entity's decision to deliver security updates using various methods and to send them monthly (newsletter) or as needed (e-mails) is appropriate for its environment, if all members of the workforce including management receive the security reminders.

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. Under the HIPAA Security Rule a security incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. (45 CFR § 164.304) • Determine how the organization will respond to a security incident. • Establish a reporting mechanism and a process to coordinate responses to the security incident. • 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? • Is there a procedure in place for reporting and handling incidents? • Has an analysis been conducted that relates reasonably anticipated threats and hazards to the organization that could result in a security incident to the methods that would be used for mitigation? • Have the key functions of the organization been prioritized to determine what would need to be restored first in the event of a disruption?[45]
2. Develop and Deploy an Incident Response Team or Other Reasonable and Appropriate Response Mechanism	• Determine if the size, scope, mission and other aspects of the organization justify the reasonableness and appropriateness of maintaining a standing incident response team. • Identify appropriate individuals to be a part of a formal incident response team, if the organization has determined that implementing an incident response team is reasonable and appropriate.	• Do members of the team have adequate knowledge of the organization's hardware and software? • Do members of the team have the authority to speak for the organization to the media, law enforcement, and clients or business partners? • Has the incident response team received appropriate training in incident response activities?
3. Develop and Implement Procedures to Respond to and Report Security Incidents	• *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*	• Has the organization determined that maintaining a staffed security incident hotline would be reasonable and appropriate? • Has the organization determined reasonable and appropriate mitigation options for security

[45] See Section 4.7, *HIPAA Standard: Contingency Plan.*
[46] See Section 4.22, *HIPAA Standard: Documentation.*

Key Activities	Description	Sample Questions
Implementation Specification (Required)	*their outcomes.* • Document incident response procedures that can provide a single point of reference to guide the day-to-day operations of the incident response team. • Review incident response procedures with staff with roles and responsibilities related to incident response, solicit suggestions for improvements, and make changes to reflect input if reasonable and appropriate. • Update the procedures as required based on changing organizational needs.[46]	incidents? • Has the organization determined that standard incident report templates to ensure that all necessary information related to the incident is documented and investigated are reasonable and appropriate? • Has the organization determined under what conditions information related to a security breach will be disclosed to the media? • Have appropriate (internal and external) persons who should be informed of a security breach been identified and a contact information list prepared? • Has a written incident response plan been developed and provided to the incident response team?
4. Incorporate Post-Incident Analysis into Updates and Revisions	• Measure effectiveness and update security incident response procedures to reflect lessons learned, and identify actions to take that will improve security controls after a security incident.	• Does the incident response team keep adequate documentation of security incidents and their outcomes, which may include what weaknesses were exploited and how access to information was gained? • Do records reflect new contacts and resources identified for responding to an incident? • Does the organization consider whether current procedures were adequate for responding to a particular security incident?
Primary Reference **Supplemental References**	• NIST SP 800-61,*Computer Security Incident Handling Guide* • NIST SP 800-14 • NIST SP 800-53	

Example:

As a Federal agency, EXHP is required to follow incident response procedures established separate from the Security Rule. EXHP has determined this additional process meets the Security Rule standard and implementation specification. In the event of a 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. When appropriate the covered entity will mitigate any harmful effects resulting from the security incident. 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. All steps in the process are carefully documented to maintain integrity of potential investigations. The documentation is also reviewed periodically to ensure responses are

appropriate and to identify operational or technological changes that can be made to prevent future incidents (§§ 164.308(a)(6)(i) & (6)(ii)).

Explanation:

The covered entity's decision to maintain existing procedures developed for compliance with other regulatory requirements is appropriate given the covered entity's circumstances, if the existing procedure allows the entity to comply with the standard and implementation specification at §§ 164.308(a)(6)(i) and (a)(6)(ii). 45 CFR § 164.308(a)(6)(i) requires a covered entity to implement policies and procedures for addressing security incidents. The required implementation specification at § 164.308(a)(6)(ii) requires covered entities to identify, respond, mitigate and document suspected or known security incidents. If it is determined that the existing procedures do not satisfy the standard and/or do not allow the entity to protect against reasonably anticipated threats and hazards to EPHI as required by § 164.306(a)(2), the procedure must be updated.

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. • Establish the organizational framework, roles, and responsibilities for this area. • Address scope, resource requirements, training, testing, plan maintenance, and backup requirements.	• What services must be provided within specified critical timeframes? – Patient treatment, for example, may need to be performed without disruption. – By contrast, claims processing may be delayed during an emergency with no long-term damage to the organization. • Have cross-functional dependencies been identified so as to determine how the failure in one system may negatively impact another one?
2. Conduct an Applications and Data Criticality Analysis[47] **Implementation Specification (Addressable)**	• *Assess the relative criticality of specific applications and data in support of other Contingency Plan components.* • Identify the activities and material involving EPHI that are critical to business operations. • Identify the critical services or operations, and the manual and automated processes that support them, involving EPHI. • Determine the amount of time the organization can tolerate disruptions to these operations, material or services (e.g., due to power outages). • Establish cost-effective strategies for recovering these critical services or processes.	• What hardware, software, and personnel are critical to daily operations? • What is the impact on desired service levels if these critical assets are not available? • What, if any, support is provided by external providers (Internet service providers [ISPs], utilities, or contractors)? • What is the nature and degree of impact on the operation if any of the critical resources are not available?

[47] This activity may be conducted as part of a larger analysis, sometimes called an impact analysis, that considers all material, services, systems, processes, and activities, including those do not involve EPHI and other elements of an organization not covered by the HIPAA Security Rule.

Key Activities	Description	Sample Questions
3. Identify Preventive Measures[48]	• Identify preventive measures for each defined scenario that could result in loss of a critical service operation involving the use of EPHI. • 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? • What is the cost associated with the preventive measures that may be considered? • Are the preventive measures feasible (affordable and practical for the environment)? • What plans, procedures, or agreements need to be initiated to enable implementation of the preventive measures, if they are necessary?
4. Develop Recovery Strategy[49]	• 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. • Ensure, if part of the strategy depends on external organizations for support, that formal agreements are in place with specific requirements stated.	• Have procedures related to recovery from emergency or disastrous events been documented? • Has a coordinator who manages, maintains, and updates the plan been designated? • Has an emergency call list been distributed to all employees? Have recovery procedures been documented? • 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. Data Backup Plan and Disaster Recovery Plan **Implementation Specifications (Both Required)**	• *Establish and implement procedures to create and maintain retrievable exact copies of EPHI.* • *Establish (and implement as needed) procedures to restore any loss of data.*	• Is there a formal, written contingency plan?[50] • Does it address both disaster recovery and data backup? [51] • Do data backup procedures exist? • Are responsibilities assigned to conduct backup activities? • Are data backup procedures documented and available to other staff?
6. Develop and Implement an Emergency Mode Operation Plan	• *Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the*	• Have procedures been developed to continue the critical functions identified in Key Activity?

[48] See Key Activities 4.7.5, *Data Backup Plan and Disaster Recovery Plan* and 4.7.6, *Develop and Implement an Emergency Mode Operation Plan*. This activity and all associated bullets in the Description and Sample Questions are part of the data backup plan, disaster recovery plan and the emergency mode operation plan implementation specifications.
[49] See Key Activities 4.7.5, *Data Backup Plan and Disaster Recovery Plan* and 4.7.6, *Develop and Implement an Emergency Mode Operation Plan*. This activity and all associated bullets in the Description and Sample Questions are part of the data backup plan, disaster recovery plan and the emergency mode operation plan implementation specifications.
[50] See Key Activity 4.7.1, *Develop Contingency Planning Policy*.
[51] See Key Activity 4.7.1, *Develop Contingency Planning Policy*.

Key Activities	Description	Sample Questions
Implementation Specification (Required)	*security of EPHI while operating in emergency mode.* • "Emergency mode" operation only involves those critical business processes that must occur to protect the security of EPHI during and immediately after a crisis situation.	• If so, have those critical functions that also involve the use of EPHI been identified? • Would different staff, facilities, or systems be needed to perform those functions? • Has the security of that EPHI in that alternative mode of operation been assured?
7. Testing and Revision Procedure **Implementation Specification (Addressable)**	• *Implement procedures for periodic testing and revision of contingency plans.* • Test the contingency plan on a predefined cycle (stated in the policy developed under Key Activity), if reasonable and appropriate. • Train those with defined plan responsibilities on their roles. • If possible, involve external entities (vendors, alternative site/service providers) in testing exercises. • Make key decisions regarding how the testing is to occur ("tabletop" exercise versus staging a real operational scenario including actual loss of capability). • 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? • Does testing lend itself to a phased approach? • Is it feasible to actually take down functions/services for the purposes of testing? • Can testing be done during normal business hours or must it take place during off hours? • If full testing is infeasible, has a "tabletop" scenario (e.g., a classroom-like exercise) been considered? • How frequently is the plan to be tested (e.g., annually)? • When should the plan be revised?
Primary Reference **Supplemental References**	• NIST SP 800-34,*Contingency Planning Guide for Information Technology Systems* • NIST SP 800-14 • NIST SP 800-18 • NIST SP 800-26 • NIST SP 800-30 • NIST SP 800-53	

Example:

Most hospitals of EXLHCP have maintained contingency plans for many years. Results of the organizational risk analysis identified that several hospitals had outdated contingency plans and two of the smaller hospitals had no contingency plan. After receiving the results of the risk analysis, EXLHCP's security official required all locations to have a contingency plan. In order to assist the hospitals in their updating or development activities the central management organization's contingency plan was made available as a template. All hospital locations must have a contingency plan with the same content provided in the template.

The purpose of the current organizational contingency plan is to protect the organization's assets from being damaged during an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) (§ 164.308(a)(7)(i)). The contingency plan contains all plans and procedures for preparing the organization for and responding to disaster and/or emergency situations. The policies and procedures in the plan match the implementation specifications of the contingency plan standard in the Security Rule.

The first section of the contingency plan is a data backup plan. The purpose of the backup plan is to create a useable exact copy of all information system data. The data backup plan includes detailed procedures for backing up all data and system files needed to restore the primary information system and workforce member network storage drives. The data backup procedures describe how to perform nightly incremental, or partial, backups and weekly full system backups. The full system backups are performed on the weekends while the system is not in use. The backup procedures provide enough detail to be implemented by anyone with basic information systems knowledge (§ 164.308(a)(7)(ii)(A)).

The next sections of the contingency plan are the disaster recovery and emergency mode operation plans. The plans include several scenarios and procedures for restoring operations and supporting information systems. The emergency mode operation plan defines procedures for system downtime of less than 12 hours. The disaster recovery plan defines procedures for system downtime of more than 12 hours. The primary goal of both plans is to maintain critical clinical processes and business operations during emergency or disaster situations. To support the goal of continued clinical processes and business operations both plans identify procedures for maintaining or restoring electronic communications and information systems while maintaining data safeguards. If data must be restored during the emergency or disaster situation, options for data restoration range from local recovery, using the emergency mode operations plan, to secondary location recovery, using the disaster plan. Any hospital locations or other offices that use information systems provided at the central management organization's data center are included in the plan. These organizations also receive copies of the plan (§§ 164.308(a)(7)(ii)(B) – (C)).

EXLHCP has determined that testing and revision of all components of the contingency plan are critical to the success of the plan. Several testing scenarios are included in the plan. One of the testing scenarios is a walkthrough or verbal review of the plan by those responsible for functions included in the plan. During this test all parties involved meet in a single room and walk through each step of the plan to determine if the restoration will be successful. Another test in the plan is a live test. During this test the primary information system is brought down and operations are restored at an alternate operating facility. During this test all connections from the alternate operating facility to other hospital locations or other offices are tested to ensure data can be accessed. Any issues discovered during these tests or during actual disaster or emergency operations are used to revise the plan. (§ 164.308(a)(7)(ii)(D))

The covered entity determined that a formalized applications and data criticality analysis is also critical to the success of the plan. The central management office and local hospitals use and maintain over 30 information systems that contain EPHI. The criticality of information systems and EPHI is different based on the clinical process or business operation the information systems and EPHI support. The formalized applications and data criticality analysis contained in the template contingency plan classifies criticality using four categories. The four categories are used to determine priority for restoration of the applications and data. The applications and data grouped in the highest category must be restored immediately to support clinical operations and business functions. The applications and data grouped in the lowest category can be restored within 1 week (§ 164.308(a)(7)(ii)(E)).

Explanation:

The covered entity's decision to require all hospital locations to have a contingency plan is appropriate based on the facts presented. The decision to provide the central management organizations current plan and supporting procedures as a template for the hospital locations that do not have a contingency plan is appropriate for its environment if the hospital locations customize the template for their specific environment. The template contingency plan addresses the standards and implementation specifications of §§ 164.306(a)(2) and 164.308(a)(7)(ii)(A) – (E). The purpose of the entity's contingency plan is to protect all data, including EPHI, from reasonably anticipated threats and hazards. This meets the requirement of § 164.306(a)(2) to ensure the protection of EPHI from reasonably anticipated threats and hazards.

As identified in the example, the content of the entity's plan does address all implementation specifications of § 164.308(a)(7). It addresses the data backup, disaster recovery, emergency mode operations, testing and revision and applications and data criticality analysis implementation specifications. The content of the plan allows the entity to create and maintain retrievable exact copies of EPHI (§ 164.308(a)(7)(ii)(A)); establishes procedures to restore any loss of data (§ 164.308(a)(7)(ii)(B)); establishes procedures to enable continuation of critical business processes for protecting the security of EPHI while operating in emergency mode (§ 164.308(a)(7)(ii)(C)); contains procedures for periodic testing and revision of all components of the contingency plan (§ 164.309(a)(7)(ii)(D)); and assesses the relative criticality of specific applications and data in support of other contingency plan components (§ 164.309(a)(7)(ii)(E)).

The contingency plan documentation will be maintained in binders. This decision may be reasonable and appropriate if the individuals responsible for implementing the contingency plan procedures at each location have access to the binders. This method of maintaining documentation is acceptable under § 164.316(b), which requires those responsible for implementing procedures to have access to the documentation. If those responsible for performing procedures in the contingency plan cannot access the procedures when needed, the method for maintaining and distributing the documentation must be revised.

4.8 Evaluation (§ 164.308(a)(8))

HIPAA Standard: *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.*

Key Activities	Description	Sample Questions
Note: This HIPAA Standard does not include any implementation specifications.	**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. • Engage external expertise to assist the internal evaluation team where additional skills and expertise is determined to be reasonable and appropriate. • 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? • How much training will staff need on security-related technical and nontechnical issues? • If an outside vendor is used, what factors should be considered when selecting the vendor, such as credentials and experience? • What is the budget for internal resources to assist with an evaluation? • What is the budget for external services to assist with an evaluation?
2. Develop Standards and Measurements for Reviewing All Standards and Implementation Specifications of the Security Rule	• Use an evaluation strategy and tool that considers all elements of the HIPAA Security Rule and can be tracked, such as a questionnaire or checklist. • Implement tools that can provide reports on the level of compliance, integration, or maturity of a particular security safeguard deployed to protect EPHI. • If available, consider engaging corporate, legal, or regulatory compliance staff when conducting the analysis. • Leverage any existing reports or documentation that may already be prepared by the organization addressing compliance, integration, or maturity of a particular security safeguard deployed to protect EPHI.	• Have management, operational, and technical issues been considered? • Do the elements of the evaluation procedure (questions, statements, or other components) address individual, measurable security safeguards for EPHI? • Has the organization determined that the procedure must be tested in a few areas or systems? • 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. • Secure management support for the evaluation process to	• If available, have staff members with knowledge of IT security been consulted and included in the evaluation team? • If penetration testing has been

Key Activities	Description	Sample Questions
	ensure participation. • Collect and document all needed information. Collection methods may include the following: – Interviews – Surveys – Outputs of automated tools, such as access control auditing tools, system logs, and results of penetration testing. • Conduct penetration testing (where trusted insiders attempt to compromise system security for the sole purpose of testing the effectiveness of security controls), if reasonable and appropriate.	determined to be reasonable and appropriate, has specifically worded, written approval from senior management been received for any planned penetration testing? • Has the process been formally communicated to those who have been assigned roles and responsibilities in the evaluation process? • Has the organization determined if an automated tool will be used to perform the evaluation process?
4. Document Results[52]	Reasonable and appropriate documentation practices will often include: • Analyze the evaluation results. • Identify security weaknesses. • Document in writing every finding and decision. • Develop security program priorities and establish targets for continuous improvement.	• Does the process support development of security recommendations? • In determining how best to display evaluation results, have written reports that highlight key findings and recommendations been considered? • If a written final report is to be circulated among key staff, have steps been taken to ensure that it 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, complexity, and environmental and/or operational changes (e.g., other relevant laws or accreditation requirements). • In addition to periodic re-evaluations, consider repeating evaluations when environmental and operational changes are made to the organization that affect the security of EPHI (e.g., 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 environmental and operational changes are made that affect the security of EPHI? • Do policies on frequency of security evaluations reflect any and all relevant Federal or state laws which bear on environmental or operational changes affecting the security of EPHI?
Primary References	• NIST SP 800-26,*Security Self-Assessment Guide for Information Technology Systems* • NIST SP800-53/FIPS 200, *Recommended Security Controls for Federal Information Systems*	

[52] See Section 4.22, *HIPAA Standard: Documentation*.

Key Activities	Description	Sample Questions
Supplemental References	• NIST SP800-14 • NIST SP800-37 • NIST SP800-55	

Example:

As part of its overall compliance plan, EXHP chose to modify its enterprise risk analysis tool to include all standards and implementation specifications of the Security Rule in question format. EXHP also included the questions from the NIST Special Publication (SP) *Security Self-Assessment Guide for Information Technology Systems* (NIST SP 800-26) in the enterprise risk analysis tool. EXHP is a Federal agency and is required to use NIST SP 800-26. The main office and all remote offices are also required to perform an evaluation of the technical and non-technical operations of each location. Results of the risk analysis and evaluation help to focus the organization's efforts to develop additional policy and procedures, mitigate security issues, and apply reasonable and appropriate security safeguards. The evaluation is performed yearly and revisited based on operational or environmental changes (§ 164.308(a)(8)).

Explanation:

The covered entity's decision to perform the evaluation by using the modified enterprise risk analysis tool is reasonable and appropriate. The evaluation standard at §164.308(a)(8) requires a covered entity to perform a periodic technical and non-technical evaluation based initially on the standards of the Security Rule and subsequently based on environmental or operational changes. If the enterprise risk analysis tool is modified to include all standards implemented under the Security Rule and is used to perform an initial and subsequent evaluations of the environment, then the approach is reasonable and appropriate.

The entity's decision to perform the evaluation every year is reasonable. The Security Rule does not define a timeframe for performing the evaluation. It states only that the evaluation must be performed periodically and in response to environmental or operational changes. If the evaluation cannot be performed on an annual or other appropriate periodic basis or in response to operational or environmental changes, the process must be revised.

4.9 Business Associate Contracts and Other Arrangements (§ 164.308(b)(1))[53]

HIPAA Standard: *A covered entity, in accordance with § 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 § 164.314(a) that the business associate will appropriately safeguard the information*[54, 55]

Key Activities	Description	Sample Questions
Note: For the definition of a "business associate," see 45 CFR §160.103 or Appendix B – Glossary of this document.	**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 or other arrangements. • Reevaluate the list of business associates to determine who has access to EPHI in order to assess whether the list is complete and current. • 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? • 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: – Claims processing or billing – Data analysis – Utilization review – Quality assurance – Benefit management – Practice management – Re-pricing – All other HIPAA-regulated functions – Hardware maintenance. • Have outsourced functions involving the use of EPHI been considered, such as the following: – Actuarial services – Data aggregation – Administrative services – Accreditation – Financial services?
2. Written Contract or Other Arrangement[56] **Implementation**	• *Document the satisfactory assurances required by this standard through a written contract or other arrangement*	• Who is responsible for coordinating and preparing the final agreement or arrangement?

[53] See Section 4.19, *HIPAA Standard: Business Associate Contracts and Other Arrangements*.
[54] (2) This standard does not apply with respect to (i) The transmission by a covered entity of EPHI to a health care provider concerning the treatment of an individual. (ii) The transmission of EPHI by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of §164.314(b) and §164.504(f) apply and are met; or (iii) The transmission of EPHI from or to other agencies providing the services at §164.502(e)(1)(ii)(C), when the covered entity is a health plan that is a government program providing public benefits, if the requirements of §164.502(e)(1)(ii)(C) are met.
[55] (3) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and §164.314(a).
[56] See also Key Activity 4.9.4, *Implement An Arrangement Other than a Business Associate Contract if Reasonable and Appropriate*.

Key Activities	Description	Sample Questions
Specification (Required)	*with the business associate that meets the applicable requirements of §164.314(a).*[57] • Execute new or update existing agreements or arrangements as appropriate. • Identify roles and responsibilities. • Include security requirements in business associate contracts/agreements to address confidentiality, integrity, and availability of EPHI. • Specify any training requirements associated with the contract/agreement or arrangement, if reasonable and appropriate.	• Does the agreement or arrangement specify how information is to be transmitted to and from the business associate?
3. Establish Process for Measuring Contract Performance and Terminating the Contract if Security Requirements Are Not Being Met[58]	• Maintain clear lines of communication. • Conduct security reviews. • Establish criteria for measuring contract performance (metrics). • If the business associate is a governmental entity, update the memorandum of understanding or other arrangement when required by law or regulation, or when reasonable and appropriate.	• What is the service being performed? • What is the outcome expected? • Is there a process for reporting security incidents related to the agreement? • 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?
4. Implement An Arrangement Other than a Business Associate Contract if Reasonable and Appropriate	• If the covered entity and its business associate are both governmental entities, use a memorandum of understanding or reliance on law or regulation that requires equivalent actions on the part of the business associate. • Document the law, regulation, memorandum, or other document that assures that the governmental entity business associate will implement all required safeguards for EPHI involved in transactions between the parties.	• Is the covered entity's business associate a federal, state, or local governmental entity? • Is there a usual procedure for creating memoranda of understanding between the parties? • Has the covered entity researched and reviewed all law and regulation governing the use of EPHI by the governmental entity business associate?
Primary References	• NIST SP 800-47,*Security Guide for Interconnecting Information Technology Systems* • NIST SP 800-35,*Guide to Information Technology Security Services*	

[57] See Section 4.19, *HIPAA Standard: Business Associate Contracts and Other Arrangements*.
[58] See Section 4.19 , *HIPAA Standard: Business Associate Contracts and Other Arrangements.*

Key Activities	Description	Sample Questions
Supplemental References	• NIST SP 800-14 • NIST SP 800-36 • NIST SP 800-53 • NIST SP 800-64	

Example:

During implementation of the HIPAA Privacy Rule, EXLHCP developed business associate contract (BAC) and memorandum of understanding (MOU) language. Each of the entity's business associates, including those using EPHI, was identified during Privacy Rule implementation. Contracts or MOUs were executed with each of the business associates or other government entities. After reviewing the requirements of § 164.314(a) the organization determined that no additional language is needed. The covered entity decided appropriate safeguard language was included in the original versions of the BAC and MOU (§§ 164.308(b)(1) & (4)).

Explanation:

The covered entity's decision not to update existing business associate agreements and memoranda of understanding language developed for Privacy Rule compliance is a permissible way of meeting the requirements of this standard. 45 CFR §164.308(b)(1) requires a covered entity to document satisfactory assurances that the business associate will meet all requirements of § 164.314(a). The entity reviewed the existing BACs and MOUs to determine if the written language appropriately addresses requirements of § 164.314(a). The decision was made that all language requirements of § 164.314(a) were addressed. If the covered entity determined the existing language does not provide satisfactory assurances that the business associate will maintain reasonable and appropriate safeguards, the language must be updated.

Physical Safeguards

4.10 Facility Access Controls (§ 164.310(a)(1))[59]

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.*

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[60, 61]	• Inventory facilities and identify shortfalls and/or vulnerabilities in current physical security capabilities. • Assign degrees of significance to each vulnerability identified and ensure proper access is allowed. • Determine which types of facilities require access controls to safeguard EPHI, such as: – Data Centers – Peripheral equipment locations – IT staff offices – Workstation locations.	• If reasonable and appropriate, do nonpublic areas have locks and cameras? • Are workstations protected from public access or viewing?[62] • Are entrances and exits that lead to locations with EPHI secured? • Do policies and procedures already exist regarding access to and use of facilities and equipment? • Are there possible natural or man-made disasters that could happen in our environment?[63] • Do normal physical protections exist? (Locks on doors, windows, etc., and other means of preventing unauthorized access.)
2. Identify Corrective Measures[64, 65]	• Identify and assign responsibility for the measures and activities necessary to correct deficiencies and ensure proper access is allowed. • Develop and deploy policies and procedures to ensure that repairs, upgrades, and /or modifications are made to the appropriate physical areas of the facility while ensuring proper access is allowed.	• Who is responsible for security?[66] • Is a workforce member other than the security official responsible for facility/physical security? • Are facility access control policies and procedures already in place? Do they need to be revised? • What training will be needed for employees to understand the policies and procedures?[67] • How will we document the decisions and actions?[68] • Are we dependent on a landlord to make physical changes to meet the requirements?

[59] See also Section 4.4, *HIPAA Standard: Information Access Management* and Section 4.14, *HIPAA Standard: Access Control.*
[60] This key activity may be performed as part of the risk analysis implementation specification. See Section 4.1, *HIPAA Standard: Security Management Process.*
[61] See Key Activity 4.10.3, *Develop a Facility Security Plan.* This activity and all associated bullets in the Description and Sample Questions are part of the facility security plan implementation specification.
[62] See Section 4.11, *HIPAA Standard: Workstation Use.*
[63] See Section 4.7, *HIPAA Standard: Contingency Plan.*

Key Activities	Description	Sample Questions
3. Develop a Facility Security Plan **Implementation Specification (Addressable)**	• *Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.* • Implement appropriate measures to provide physical security protection for EPHI in a covered entity's possession. • Include documentation of the facility inventory, as well as information regarding the physical maintenance records and the history of changes, upgrades, and other modifications. • Identify points of access to the facility and existing security controls.	• Is there an inventory of facilities and existing security practices? • What are the current procedures for securing the facilities (exterior, interior, equipment, access controls, maintenance records, etc.? • Is a workforce member other than the security official responsible for the facility plan? • Is there a contingency plan already in place, under revision, or under development?[69]
4. Develop Access Control and Validation Procedures **Implementation Specification (Addressable)**	• *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.* • Implement procedures to provide facility access to authorized personnel and visitors, and exclude unauthorized persons.	• What are the policies and procedures in place for controlling access by staff, contractors, visitors, and probationary employees? • How many access points exist in each facility? Is there an inventory? • Is monitoring equipment necessary?
5. Establish Contingency Operations Procedures **Implementation Specification (Addressable)**	• *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.*	• Who needs access to EPHI in the event of a disaster? • What is the backup plan for access to the facility and/or EPHI? • Who is responsible for the contingency plan for access to EPHI? • Who is responsible for implementing the contingency plan for access to EPHI in each department, unit, etc.? • Will the contingency plan be appropriate in the event of all types of potential disasters (Fire, flood, earthquake, etc.)?
6. Maintain Maintenance	• *Implement policies and procedures to document repairs*	• Are records of repairs to hardware, walls, doors and locks

[64] This key activity may be performed as part of the risk management implementation specification. See Section 4.1, *HIPAA Standard: Security Management Process.*
[65] See Key Activity 4.10.3, *Develop a Facility Security Plan.* This activity and all associated bullets in the Description and Sample Questions are part of the facility security plan implementation specification.
[66] See Section 4.2, *HIPAA Standard: Assigned Security Responsibility.*
[67] See Section 4.5, *HIPAA Standard: Security Awareness and Training.*
[68] See Section 4.22, *HIPAA Standard: Documentation.*
[69] See Section 4.7, *HIPAA Standard: Contingency Plan.*

Key Activities	Description	Sample Questions
Records **Implementation Specification (Addressable)**	*and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors and locks).*	maintained? • Has responsibility for maintaining these records been assigned?
Supplemental References	• NIST SP 800-14 • NIST SP 800-18 • NIST SP 800-26 • NIST SP 800-30 • NIST SP 800-34 • NIST SP 800-53	

Example:

EXHP has several layers of facility safeguards and access controls at each location. The main office developed the facility access controls policy that the covered entity decided will allow them to meet this standard. The entity's policy requires appropriate access controls to the exterior and interior of all physical locations. The policy includes provisions requiring all workforce members to display ID badges and visitors to be escorted by an authorized workforce member in all work areas. If a workforce member is prevented access to a physical location, procedures exist to verify they are authorized to access the location. Each of the remote offices is responsible for implementing procedures that adhere to policy developed by the main office. To ensure all offices use appropriate safeguards, the main office established standards for physical access control measures. The most common measure used by the offices is a card reader access control system for all areas workforce members need to access. Different access levels were established based on the job classification activities pursuant to §§ 164.310(a)(1), (2)(ii) and (2)(iii).

The facility policy also required appropriate access controls to be maintained during contingency operations related to the disaster recovery or emergency operations plans. Each of the offices established procedures to maintain access controls to the facilities while permitting authorized access to those individuals responsible for recovery of operations and data. The entity decided to include this information in the Contingency Plan to ensure it would be used at the appropriate time (§ 164.310(a)(2)(i)).

EXHP's facility access controls policy also requires that any security related repairs made to any facility or component of the facility be documented. The covered entity decided it was reasonable to track any modifications, repairs or removal of physical safeguards for the facility. This section of the policy mirrors the specifications identified in the Security Rule. Each office has responsibility for implementing the procedures to document the activities. Most offices use an electronic tracking form. Other locations capture the modifications on a paper form because the maintenance is not often performed. The main office has determined that either option for tracking modifications, repairs or removal of physical safeguards is acceptable (§ 164.310(a)(2)(iv)).

Explanation:

The covered entity's decision to maintain the existing policies and procedures for facility access controls is reasonable and appropriate. The entity determined that the standards and implementation specifications at §§ 164.310(a)(1), (a)(2)(ii), and (a)(2)(iii) are all addressed in the current policy and procedures. The facility access controls standard at § 164.310(a)(1) requires covered entities to implement policies and procedures to limit physical access to information system and facilities where the information systems are housed, while ensuring authorized access is allowed. The addressable implementation specification at § 164.310(a)(2)(ii) for a facility security plan requires covered entities to assess whether to implement

policies and procedures to safeguard the facility and equipment from unauthorized physical access, tampering, and theft. The addressable implementation specification at § 164.310(a)(2)(iii) for access control and validation procedures requires a covered entity to assess whether to implement policies and procedures to control and validate a person's access to facilities based on their role or function, including visitor controls. The entity has determined that the existing policies and procedures will allow them to limit or reduce unauthorized physical access, allow authorized access, safeguard the facility and equipment therein and control and validate authorized access to the facilities and locations where information systems exist. If the policy, procedures or security measures used do not appropriately address this standard or implementation specifications they must be revised.

The covered entity's decision to allow all remote offices to develop access control procedures to be used during contingency operations and to include this information in the Contingency Plan a permissible way of meeting the requirements of this standard. The addressable implementation specification at § 164.310(a)(2)(i) for contingency operations requires a covered entity to determine whether to establish procedures for allowing facility access to support data restoration during an emergency and to implement the procedures as needed. The entity has decided to implement this specification by developing contingency operations procedures at all locations and combining the procedures into the Contingency Plan. The Security Rule does not identify how the procedures should be documented or maintained. 45 CFR § 164.316(b)(2)(ii) only requires the documentation to be available to those persons responsible for implementing the procedures. Inclusion of the procedures in the Contingency Plan should ensure that the procedures will be available to those responsible for implementation, if needed. If the procedures do not support facility access during data restoration or are not available if needed, then the procedures and location where they are maintained must be revised.

The covered entity's decision to track all modifications, repairs or removal of physical safeguards for the facility is reasonable and appropriate. 45 CFR § 164.310(a)(2)(iv) requires covered entities to assess whether implementation of 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) is reasonable and appropriate for their environment. The entity's determination that the current policies and procedures for facility access controls contain the processes needed to meet this addressable implementation specification is appropriate for its environment. If the policy and procedures do not address documentation of maintenance and repairs to physical security components of the facility, the documentation must be revised.

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
Note: This HIPAA Standard does not include any implementation specifications.	**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. • 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). • 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? • Who is responsible for this inventory and its maintenance? • What tasks are commonly performed on a given workstation or type of workstation? • Are all types of computing devices used as workstations identified along with the use of these workstations?
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? • What are key operational risks that could result in a breach of security?
3. Analyze Physical Surroundings for Physical Attributes[70]	• Ensure that any risks associated with a workstation's surroundings are known and analyzed for possible negative impacts. • 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? • Is viewing by unauthorized individuals restricted or limited at these workstations? • Do changes need to be made in the space configuration? • Do employees understand the security requirements for the data they use in their day-to-day jobs?
Supplemental References	• NIST SP 800-14 • NIST SP 800-53	

Example:

EXLHCP has existing formal Workstation Acceptable Use policy and procedures identifying the proper functions to be performed on workstations. The policy and procedures identify the attributes of the physical surroundings of an information system and the appropriate safeguards to be implemented on the workstations. The procedures section also includes guidelines for manual protection of workstations to be practiced by all workforce members. These safeguards are discussed further in the Section 4.12, *Workstation Security*. The entity has determined the existing policy and procedures meet Security Rule compliance and no revisions are needed (§ 164.310(b)).

[70] See Section 4.5, *HIPAA Standard: Security Awareness and Training.* This key activity should be performed during security training or awareness activities.

Explanation:

The covered entity's decision to use the existing Workstation Acceptable Use policy a permissible way of meeting the requirements of this standard. The standard for workstation security at § 164.310(b) requires a covered entity to implement policies and procedures that specify the proper functions and manner in which the functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI. The entity's existing workstation acceptable use policy and procedures identify proper functions to be performed, the attributes of the physical surroundings and appropriate safeguards to be implemented on all information systems, including those with EPHI. If the policy does not meet the requirements of § 164.310(b), and thus does not enable the covered entity to comply with the standards or establishes insufficient workstation security safeguards, the policy must be revised.

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
Note: This HIPAA Standard does not include any implementation specifications.	**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? • Are any workstations located in public areas? • Are laptops used as workstations?
2. Analyze the Risk Associated with Each Type of Access[71]	• Determine which type of access holds the greatest threat to security.	• Are any workstations in areas that are more vulnerable to unauthorized use, theft or viewing of the data they contain? • What are the options for making modifications to the current access configuration?
3. Identify and Implement Physical Safeguards for Workstations	• Implement physical safeguards and other security measures to minimize the possibility of inappropriate access to EPHI through workstations.	• What safeguards are in place i.e. locked doors, screen barriers, cameras, guards?[72] • Do any workstations need to be relocated to enhance physical security? • Have employees been trained on security?[73]
Supplemental References	• NIST SP 800-14 • NIST SP 800-53	

Example:

EXLHCP's Workstation Use policy established the safeguards to be used to secure workstations. The purpose of the physical safeguards is to restrict access to authorized users. Each hospital documents the procedures implemented in their environment to safeguard workstations. The primary safeguard implemented at all locations to restrict access to the hospital data center is a card reader access control system. Only authorized employees with access cards are able to access the data center locations. Additional safeguards that are implemented for areas with visitors include positioning of workstation monitors away from open areas and using password protected screen savers or requiring employees to lock workstations before leaving them. (§ 164.310(c))

Explanation:

The covered entity's decision to implement multiple levels of safeguards to protect workstations from unauthorized access is a permissible way of meeting the requirements of this standard. The entity's

[71] This key activity may be conducted pursuant to the risk analysis and risk management implementation specifications of the security management process standard. See Section 4.1, *HIPAA Standard: Security Management Process.*
[72] See Section 4.1, *HIPAA Standard: Security Management Process.*
[73] See Section 4.5, *HIPAA Standard: Security Awareness and Training.*

workstation acceptable use policy and the requirements of §164.310(c) require implementation of physical safeguards for all workstations that access EPHI to restrict access to authorized users. The decisions to implement safeguards such as the card reader access control system, positioning of workstation monitors and using password-protected screensavers are all reasonable given the covered entity's circumstances. The Security Rule does not require the use of specific security measures to comply with this standard. The Security Rule general rules regarding flexibility of approach at § 164.306(b)(1) does allow all covered entities to use any security measures that allow it to reasonably and appropriately implement the standards and implementation specifications of the Security Rule for its environment. If the physical safeguards implemented by each hospital location do not allow the entity to meet the requirements of the Workstation Acceptable Use policy and the workstation security standard at § 164.310(c), additional or new safeguards must be implemented.

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. Implement Methods for Final Disposal of EPHI. **Implementation Specification (Required)**	• *Implement policies and procedures to address the final disposition of EPHI, and/or the hardware or electronic media on which it is stored.* • Determine and document the appropriate methods to dispose of hardware, software, and the data itself. • Assure that EPHI is properly destroyed and cannot be recreated.	• What data is maintained by the organization, and where? • Is data on removable, reusable media such as tapes and CDs? • Is there a process for destroying data on hard drives and file servers? • What are the options for disposing of data on hardware? What are the costs?
2. Develop and Implement Procedures for Reuse of Electronic Media **Implementation Specification (Required)**	• *Implement procedures for removal of EPHI from electronic media before the media are made available for re-use.* • Ensure that EPHI previously stored on electronic media cannot be accessed and reused. • Identify removable media and their use. • Ensure that EPHI is removed from reusable media before they are used to record new information.	• Do policies and procedures already exist regarding reuse of electronic media (hardware and software)? • Is one individual and/or department responsible for coordinating the disposal of data, and the reuse of the hardware and software? • Are employees appropriately trained on security and risks to EPHI when reusing software and hardware?[74]
3. Maintain Accountability for Hardware and Electronic Media **Implementation Specification (Addressable)**	• *Maintain a record of the movements of hardware and electronic media and any person responsible therefore.* • Ensure that EPHI is not inadvertently released or shared with any unauthorized party. • 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)? • What procedures already exist regarding tracking of hardware and software within the company? • If workforce members are allowed to remove electronic media that contain or may be used to access EPHI, do procedures exist to track the media externally? • Who is responsible for maintaining records of hardware and software?
4. Develop Data Backup and Storage Procedures **Implementation Specification**	• *Create a retrievable, exact copy of EPHI, when needed, before movement of equipment.* • Ensure that an exact, retrievable copy of the data is retained and protected to protect the integrity	• Are backup files maintained offsite to assure data availability in the event data is lost while transporting or moving electronic media containing EPHI?

[74] See Section 4.5, *HIPAA Standard: Security Awareness and Training.*

Key Activities	Description	Sample Questions
(Addressable)	protected to protect the integrity of EPHI during equipment relocation.	• If data were to be unavailable while media are transported or moved for a period of time, what would the business impact be?
Primary Reference **Supplemental References**	• NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems* • NIST SP 800-34 • NIST SP 800-53	

Example:

EXHP has established new organization-wide policy and procedures for device and electronic media controls. The policy and procedures identify proper steps for receipt, removal and movement of all electronic media both internal and external to the facility. The policy states the organization's position on disposal, media re-use, accountability and data backup and storage. All locations follow this policy and procedures (§ 164.310(d)(1)).

The policy states that all data on electronic media must be properly destroyed prior to disposal or removal from the organization. Each location is responsible for implementing standard procedures for the destruction and disposal of electronic media. All workforce members that dispose of electronic media must bring the data to the IS department. The IS department then disposes of the data. The covered entity's procedure requires the use of a special mechanical device to physically destroy the media before disposal. If needed, remote offices are provided with the option to use a business associate to perform the physical destruction. If this method is used, the destruction must be performed at the remote office location (§ 164.310(d)(2)(i)).

EXHP's Device and Electronic Media Controls policy states that if electronic media is to be reused within the organization it must be properly overwritten or erased before the media is made available for re-use. As with the disposal procedure, the IS department at each location is responsible for this procedure. The organizational procedure for making media available for re-use includes the use of a special software program to overwrite data at the hardware level. The main office evaluated and purchased the program to perform this function. The program is distributed to all offices for local use. After the program is run on the media and erasure of data has been confirmed, it is made available for re-use and distributed to the new location by the IS department. (§ 164.310(d)(2)(ii))

The entity's policy identifies each department manager and the IS department as being accountable for movement of electronic media. The accountability procedure requires the use of an inventory and tracking database developed by the main office. The IS department is accountable for the first steps in the process. These steps include identifying all electronic media with an identifying label, and inventorying the electronic media in the tracking database. Once the media is moved to a department, the accountability is shared between the IS department and the department manager. IS updates the database with the location of the media and the responsible department manager. The department manager is responsible for periodically checking on the media assigned to their department. The spot check is performed to ensure media has not been moved to a different location or removed from the facility (§ 164.310(d)(2)(iii)).

If media is moved, organizational policy requires that the IS department ensures that any data stored on the media is properly backed up before movement. The primary backup procedure only addresses the backup of the primary information system and workforce member network storage drives. This procedure

focuses on the movement of workforce member workstations that are used to store EPHI. Workforce members are able to store data, including EPHI, on workstations but data stored on workstations is not backed up in the network backup process. The procedure allows the IS department to temporarily store the data on the network or use a portable writable CD-ROM drive for the backup. Immediately after the device is moved, the data is restored to the workstation (§ 164.310(d)(2)(iv)).

EXHP's risk analysis identified disposal, re-use and accountability issues with the multiple forms of portable media. To mitigate these risks the covered entity decided to restrict the use of portable media. The restriction is documented in the device and electronic media controls policy. The only approved portable media are CD-ROMs and floppy disks. The covered entity chose to eliminate the use of all other portable media. All workforce members have the ability to use floppy disks. Workforce members must submit a request for writeable CD-ROM drives. Only workforce members approved by the Security Official or Security Committee are authorized to have writeable CD-ROM drives. This includes approval of members of the IS department (§ 164.310(d)(2)(iii)).

Explanation:

The covered entity's decision to implement a new policy and procedure for device and media controls is appropriate under the entity's circumstances. The entity is required by § 164.310(d)(1) to 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.

The entity's decision to establish standard procedures for disposal of electronic media containing PHI to comply with the media controls policy and the implementation specification at § 164.310(d)(2)(i) and to allow each location to implement the procedures is reasonable and appropriate in the covered entity's circumstances. The required implementation specification at § 164.310(d)(2)(i) states that covered entities must 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. This specification does not prohibit the entity from assigning the IS department or a business associate to conduct the disposal procedure. If a business associate is used to perform EPHI disposal, a business associate contract with assurances that appropriate safeguards will be implemented, as required by §§ 164.308(b)(1) and 164.314(a), must also be implemented. If the procedure used does not properly dispose of electronic media with PHI or if the business associate does not provide satisfactory assurances of security safeguards related to the EPHI, the procedure and methods for disposal must be changed.

The covered entity's decision to implement special data erasing programs to ensure any EPHI is overwritten or erased prior to media being re-used is appropriate for its environment. 45 CFR § 164.310(d)(2)(ii) requires a covered entity to implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use. The policy, procedures and security measure implemented by the entity reasonably address this requirement. If the procedures or security measure do not allow the entity to properly remove data before re-use, it must be revised.

The covered entity's decision to make both department managers and the IS department at each remote office accountable for movement of electronic media with PHI using an inventory and tracking database is appropriate under the covered entity's circumstances. The addressable implementation specification at § 164.310(d)(2)(iii) for accountability requires a covered entity to assess whether it is reasonable and appropriate to maintain a record of the movements of hardware and electronic media and any person responsible therefore. This specification does not prohibit a covered entity from assigning this function to multiple departments or requiring the use of a specific tracking mechanism, such as the inventory and

tracking database implemented by this entity. This process might not be reasonable and appropriate if the IS department did not maintain the tracking database, or information is not shared between the departments, or if each department manager does not check on the media assigned to their department.

The covered entity's decision to back up all electronic media, including media with PHI, before movement of the media is appropriate in this covered entity's environment. The addressable implementation specification at § 164.310(d)(2)(iv) requires a covered entity to assess whether it is reasonable and appropriate to create a retrievable, exact copy of EPHI, when needed, before movement of equipment. The entity's decision to use the Backup Plan in the Contingency Plan to make retrievable, exact copies of EPHI on the primary information system and network storage drives is appropriate under these circumstances. In addition, the decision to develop this procedure to focus on making retrievable, exact copies of EPHI stored on a workstation before moving the workstation is also appropriate. The procedures established to meet this implementation specification would likely not be reasonable and appropriate if retrievable copies of the EPHI could not be created for this covered entity.

The entity's decision to implement an additional policy restricting the use of certain electronic media is reasonable and appropriate under these facts. If the entity's risk analysis identifies threats to the security or integrity of EPHI that may be stored on certain portable media, the entity must implement security measures sufficient to reduce the risk to a reasonable and appropriate level to comply with the general security requirements of § 164.306(a).

Technical Safeguards

4.14 Access Control (§ 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 § 164.308(a)(4)*[75].

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[76]	• Identify an approach for access control. • Consider all applications and systems containing EPHI that should only be available to authorized users. • Integrate these activities into the access granting and management process.[77]	• Have all applications/systems with EPHI been identified? • What user roles are defined for those applications/systems? • Where is the EPHI supporting those applications/systems currently housed (e.g., stand-alone PC, network)? • Are data and/or systems being accessed remotely?
2. Identify Technical Access Control Capabilities	• Determine the access control capability of all information systems with EPHI.	• How are the systems accessed (viewing data, modifying data, creating data)?
3. Ensure that All System Users Have Been Assigned a Unique Identifier **Implementation Specification (Required)**	• *Assign a unique name and/or number for identifying and tracking user identity.* • Ensure that system activity can be traced to a specific user. • Ensure that the necessary data is available in the system logs to support audit and other related business functions.[78]	• How should the identifier be established (length and content)? • Should the identifier be self-selected or randomly generated?
4. Develop Access Control Policy[79]	• Establish a formal policy for access control that will guide the development of procedures.[80] • Specify requirements for access control that are both feasible and cost-effective for implementation.[81]	• Have rules of behavior been established and communicated to system users? • How will rules of behavior be enforced?

[75] Note: This HIPAA standard supports the standards at Section 4.4, *Information Access Management* and Section 4.10, *Facility Access Controls*.
[76] See Section 4.4, *HIPAA Standard: Information Access Management.* This activity and all associated bullets in the Description and Sample Questions should be conducted as part of the access granting and access establishment process detailed in the Information Access Management standard.
[77] See Section 4.4, *HIPAA Standard: Information Access Management.*
[78] See Section 4.15, *HIPAA Standard: Audit Control.*
[79] See Section 4.4, *HIPAA Standard: Information Access Management.*
[80] See Section 4.4, *HIPAA Standard: Information Access Management.*
[81] See Section 4.1, *HIPAA Standard: Security Management Process.*

Key Activities	Description	Sample Questions
5. Implement Access Control Procedures Using Selected Hardware and Software	• Implement the policy and procedures using existing or additional hardware/software solution(s).	• Who will manage the access controls procedures? • Are current users trained in access control management?[82] • 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.[83] • Determine if any changes are needed for access control mechanisms. • Establish procedures for updating access when users require the following:[84] – Initial access. – Increased access. – Access to different systems or applications than those they currently have.	• Have new employees/users been given proper instructions for protecting data and systems?[85] • What are the procedures for new employee/user access to data and systems?[86] • Are there procedures for reviewing and, if appropriate, modifying access authorizations for existing users?[87]
7. Establish an Emergency Access Procedure **Implementation Specification (Required)**	• *Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.* • 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? • Who is authorized to make the decision?[88] • Who has assigned roles in the process?[89] • Will systems automatically default to settings and functionalities that will enable the emergency access procedure or will the mode be activated by the system administrator or other authorized individual?
8. Automatic Logoff and Encryption and Decryption **Implementation Specifications (Both Addressable)**	• Consider whether the addressable implementation specifications of this standard are reasonable and appropriate: – *Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.* – *Implement a mechanism to encrypt and decrypt EPHI.*	• Are automatic logoff features available for any of the covered entity's operating systems or other major applications? • If applications have been created or developed in-house, is it reasonable and appropriate to modify them to feature automatic logoff capability? • What period of inactivity prior to automatic logoff is reasonable and appropriate for the covered entity? • What encryption systems are available for the covered entity's EPHI?

[82] See Section 4.5, *HIPAA Standard: Security Awareness and Training.*
[83] See Section 4.4, *HIPAA Standard: Information Access Management.*
[84] See Section 4.4, *HIPAA Standard: Information Access Management.*
[85] See Section 4.5, *HIPAA Standard: Security Awareness and Training.*
[86] See Section 4.4, *HIPAA Standard: Information Access Management.*
[87] See Section 4.4, *HIPAA Standard: Information Access Management.*
[88] See Section 4.7, *HIPAA Standard: Contingency Plan.*
[89] See Section 4.7, *HIPAA Standard: Contingency Plan.*

Key Activities	Description	Sample Questions
		• Is encryption appropriate for storing and maintaining EPHI ("at rest"), as well as while it is transmitted?
9. Terminate Access if it is No Longer Required[90]	• Ensure access to EPHI is terminated if the access is no longer authorized.	• 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 References	• NIST SP 800-14 • NIST SP 800-53 • NIST SP 800-56 • NIST SP 800-57 • NIST SP 800-63 • FIPS 140-2	

Example:

EXHP establishes access to the primary information system using the Information Access Management policy and procedures identified in the previous Administrative Safeguards examples. The Intranet based application described in the Administrative Safeguards example sends an e-mail to the IS department to establish access. The IS department has developed a technical policy and procedure for providing access to the system. The policy requires that only an authorized IS system administrator can perform access functions in the system. The procedure provides a step-by-step guide that system administrators use to perform access functions. EXHP's risk analysis and evaluation of the information system verified that appropriate access controls are available and users can be segmented from different PHI based on their job classifications. Each of the pre-authorized access levels, defined in the Intranet application, is matched to a template in the system that defines certain functions the user can perform (§ 164.312(a)(1)).

The access control policy requires that all users be assigned a unique user name for all applications. Using their unique name and a password, assigned for user authentication, the users only obtain access to PHI needed for their job functions. The entity's procedure for assigning user names defines the standard characteristics, or naming convention, of the user name. The entity's standard for user names is first letter of first name, first two letters of last name and a random four-digit number (e.g., FLL4321) (§ 164.312(a)(2)(i)).

EXHP identified emergency situations in the past when access to the information system was needed but not provided in a timely manner. A procedure for handling these instances was developed. The procedure defines situations that constitute an emergency. One type of emergency situation addressed in the procedure is not being able to grant immediate access to new workforce members, such as temporary employees, that are exceptions to the standard access establishment procedures. This emergency situation is addressed in new procedures established for implementation of the new Intranet based workforce access workflow system, which will automate the section of the procedure requiring immediate granting of access during emergencies. Another emergency situation addressed in the procedure is when the information system is unavailable. EXHP determined that, if an emergency occurred making the system unavailable, the Contingency Plan procedures would be used to continue business operations and provide access to EPHI (§ 164.312(a)(2)(ii)).

[90] See Section 4.3, *HIPAA Standard: Workforce Security.*

EXHP has a Workstation Acceptable Use policy that requires all workstations to have automatic logoff capabilities. The procedures implemented to safeguard workstations include password protected screen savers or workstation locking. EXHP determined that additional logoff capabilities were needed at the information system level. The system has the capability to electronically enforce a logoff function at a determined time interval of inactivity. The time interval is set at 5 minutes. This is consistent with the workstation time interval. If the time interval is exceeded, the user must re-authenticate to the computer with their unique user name and password (§ 164.312(a)(2)(iii)).

Finally, after performing the risk analysis, EXHP decided to encrypt and decrypt all data in the information system. The information system has the capability to perform these functions using a strong form of encryption. Due to system performance considerations the entity determined that data would only be encrypted during non-work hours. Each evening the database is encrypted and each morning it is decrypted (§ 164.312(a)(2)(iv)).

Explanation:

The covered entity's decision to implement technical access control policies and procedures based on the information access management standard at § 164.308(a)(4) and technical capabilities of the primary information system a permissible way of meeting the requirements of this standard. 45 CFR § 164.312(a)(1) requires a covered entity to implement technical policies and procedures for information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4). The access rights to EPHI established in the entity's information access management policy are based on a workforce member's job function. The technical capabilities of the information system do allow for segmentation of access to the EPHI based on the job functions established in the information access management policy. The technical procedures established to implement the information access management policy would not be reasonable and appropriate if the information system was not capable of segmenting access to EPHI based on the job classifications defined in the policy.

The covered entity's decision to assign all users of the information system a unique user name using a standard naming convention that uniquely identifies each user to the information system is appropriate given the covered entity's circumstances. The implementation specification at § 164.312(a)(2)(i) requires covered entities to assign a unique name and/or number for identifying and tracking user identity. The Security Rule does not specify the naming convention, or format for the unique user name as long as each user can be uniquely identified from other information system users. The naming convention for assigning user names would not be reasonable and appropriate if users could not be distinguished from each other when accessing the information system (e.g. shared or generic user names).

The covered entity's decision to identify different situations when emergency access to information systems with EPHI is needed and to implement the procedures in those identified situations is reasonable and appropriate. The implementation specification at § 164.312(a)(2)(ii) requires a covered entity to establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. The entity's decision to define the emergency situations to mean immediate access is needed for certain types of workforce members or during emergency situations when the Contingency Plan is activated is reasonable and appropriate. This procedure would not be reasonable and appropriate if it does not account for all types of access to be established for users during emergency situations. If additional emergency situations are identified, the procedure must be revised.

The covered entity's decision to use the existing capabilities of the information system to supplement the automatic logoff procedures implemented under the Workstation Acceptable Use policy is appropriate for

its environment. The addressable implementation specification at § 164.312(a)(2)(iii) requires covered entities to determine whether to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. The Security Rule does not identify the duration of the predetermined time of inactivity; therefore, the entity's decision to set the time interval at 5 minutes is acceptable if the entity has determined this time interval is reasonable and appropriate for its environment. This process would not be reasonable and appropriate if the automatic logoff capability was implemented but the predetermined time of inactivity was set for a duration of time that would not trigger the automatic logoff feature in a reasonable amount of time, such as eight hours.

The covered entity's decision to only implement encryption and decryption of data in the primary information system during non-business hours is appropriate for this covered entity. The addressable implementation specification at §164.312(a)(2)(iv) requires covered entities to determine whether to implement a mechanism to encrypt and decrypt EPHI. To determine whether to implement encryption the entity reviewed the results of the risk analysis associated risk management options and technical capabilities of the information system. After reviewing these sources of information the entity concluded that encryption and decryption of EPHI in the information system during normal business hours would not reduce risk levels but would decrease system performance. The entity also concluded that implementing the system capabilities for encryption during non-business hours would not decrease system performance and would increase the security of EPHI in the information system. The decision not to implement encryption mechanisms during business hours would not be reasonable and appropriate if using these mechanisms would significantly reduce the risks to EPHI and system performance would not suffer.

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
Note: This HIPAA Standard does not include any implementation specifications.	**Introductory Reference:** *An Introduction to Computer Security: The NIST Handbook (NIST Special Publication 800-12 – Chapter 18)*	
1. Determine the Activities that Will Be Tracked or Audited	• Determine the appropriate scope of audit controls that will be necessary in information systems that contain or use EPHI based on the covered entity's risk assessment and other organizational factors .[91] • Determine what data needs to be captured.	• Where is EPHI at risk in the organization?[92] • What systems, applications, or processes make data vulnerable to unauthorized or inappropriate tampering, uses, or disclosures?[93] • What activities will be monitored (e.g., creation, reading, updating, and/or deleting of files or records containing EPHI)? • 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? • What are the most appropriate monitoring tools for the organization (third party, freeware, or operating system-provided)? • Are changes/upgrades to information systems reasonable and appropriate?
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.[94]	• Who is responsible for the overall audit process and results? • How often will audits take place? • How often will audit results be analyzed? • What is the organization's sanction policy for employee violations?[95] • Where will audit information reside (i.e., separate server)?
4. Develop Appropriate Standard Operating Procedures[96]	• 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? • Where will monitoring reports be filed and maintained? • Is there a formal process in place to address system misuse, abuse, and fraudulent

[91] See Section 4.14, *HIPAA Standard: Access Control* and Key Activity 4.1.7, *Develop and Deploy the Information System Activity Review Process.*
[92] See Section 4.1, *HIPAA Standard: Security Management Process.*
[93] See Section 4.1, *HIPAA Standard: Security Management Process.*
[94] See Section 4.1, *HIPAA Standard: Security Management Process.*
[95] See Section 4.1, *HIPAA Standard: Security Management Process.*

Key Activities	Description	Sample Questions
		activity?[97] • How will managers and employees be notified, when appropriate, regarding suspect activity?
5. Implement the Audit/System Activity Review Process[98]	• Activate the necessary audit system. • Begin logging and auditing procedures.	• What mechanisms will be implemented to assess the effectiveness of the audit process (metrics)? • What is the plan to revise the audit process when needed?
Supplemental References	• NIST SP 800-14 • NIST SP 800-53	

Example:

EXLHCP performed an evaluation of the audit controls in its 30+ information systems and identified a wide range of recording and reporting capabilities. To test the audit controls of the information systems, IS departments at all locations implemented all levels of audit controls. In many cases implementing all levels of audit controls made the systems unusable. Knowing full audit controls would not meet business needs, the audit issue was raised to the Information Security Committee. During a series of meetings the Information Security Committee decided a balance was needed between system performance and audit capabilities implemented. The committee determined audit controls would be based on business needs. Different levels of audit recording and reporting were needed to properly track information system activity. During this process the information system activity review procedures were developed. As explained earlier in this example, the requirement in this procedure is to review reports of system activity at least twice weekly. A sub-committee, consisting of IS and operational department representatives, was established to determine auditing levels. The ability to meet requirements outlined in the information system activity review procedure was a factor during development of auditing level recommendations. The sub-committee's recommendations were then turned over to IS to implement (§ 164.312(b)).

Explanation:

The covered entity's decision to use different levels of audit controls in information systems with EPHI based on varying audit control capabilities and business needs to support the information system activity review procedure is reasonable and appropriate. 45 CFR § 164.312(b) requires covered entities to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. The Security Rule does not specify the level of audit controls to implement. Therefore the entity's decision to implement different levels of audit controls to record and examine system activity ranging from detailed audit controls (all access or views of EPHI) to general audit controls (only changes to EPHI) is reasonable and appropriate. The procedural mechanisms implemented would not be reasonable and appropriate if the information systems do not have the capabilities to record and examine system activity needed for the entity's information system activity review procedures and no additional procedural mechanisms were implemented to supplement the lack of technical capabilities in the systems.

[96] See Section 4.1, *HIPAA Standard: Security Management Process.*
[97] See Section 4.1, *HIPAA Standard: Security Management Process.*
[98] See Section 4.1, *HIPAA Standard: Security Management Process.*

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 EPHI[99]	• Identify all approved users with the ability to alter or destroy data, if reasonable and appropriate. • Address this Key Activity in conjunction with the identification of unauthorized sources in Key Activity 2, below.	• How are users authorized to access the information?[100] • Is there a sound basis established as to why they need the access?[101] • Have they been trained on how to use the information?[102] • Is there an audit trail established for all accesses to the information?[103]
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 EPHI by unauthorized sources (e.g., hackers, disgruntled employees, business competitors).[104] • Conduct this activity as part of your risk analysis.[105]	• What are likely sources that could jeopardize information integrity?[106] • What can be done to protect the integrity of the information when it is residing in a system (at rest)? • What procedures and policies can be established to decrease or eliminate alteration of the information during transmission (e.g., encryption)?[107]
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? • Have the requirements been documented? • Has a written policy been developed and communicated to system users?
4. Implement Procedures to Address These Requirements	• Identify and implement methods that will be used to protect the information from modification. • Identify and implement tools and techniques to be developed or	• Are current audit, logging, and access control techniques sufficient to address the integrity of the information? • If not, what additional

[99] See Section 4.3, *HIPAA Standard: Workforce Security*, Section 4.3, *HIPAA Standard: Access Control*, and Section 4.21, *HIPAA Standard: Policies and Procedures.*
[100] See Section 4.3, *HIPAA Standard: Workforce Security* and Section 4.3, *HIPAA Standard: Access Control.*
[101] See Section 4.3, *HIPAA Standard: Workforce Security.*
[102] See Section 4.5, *HIPAA Standard: Security Awareness and Training.*
[103] See Section 4.15, *HIPAA Standard: Audit Controls.*
[104] See Section 4.1, *HIPAA Standard: Security Management Process.*
[105] See Section 4.1, *HIPAA Standard: Security Management Process.*
[106] See Section 4.1, *HIPAA Standard: Security Management Process.*
[107] See Section 4.1, *HIPAA Standard: Security Management Process.*

Key Activities	Description	Sample Questions
	procured that support the assurance of integrity.	techniques can we apply to check information integrity (e.g., quality control process, transaction and output reconstruction)? • Can additional training of users decrease instances attributable to human errors?
5. Implement a Mechanism to Authenticate EPHI **Implementation Specification (Addressable)**	• *Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.* • Consider possible electronic mechanisms for authentication such as: – Error-correcting memory – Magnetic disk storage – Digital signatures – Check sum technology	• Are the use of both electronic and non-electronic mechanisms necessary for the protection of EPHI? • Are appropriate electronic authentication tools available? • Are available electronic authentication tools interoperable with other applications and system components?
6. Establish a Monitoring Process To Assess How the Implemented Process Is Working	• Review existing processes to determine if objectives are being addressed.[108] • Reassess integrity processes continually as technology and operational environments change to determine if they need to be revised.[109]	• Are there reported instances of information integrity problems and have they decreased since integrity procedures have been implemented?[110] • Does the process, as implemented, provide a higher level of assurance that information integrity is being maintained?
Primary Reference **Supplemental References**	• NIST SP 800-14,*Generally Accepted Principles and Practices for Securing Information Technology Systems* • NIST SP 800-42 • NIST SP 800-44 • NIST SP 800-53	

Example:

While performing the most recent risk analysis process, the covered entity identified potential data integrity issues in the primary information system. The information system does have technical mechanisms to check the integrity of data and correct certain types of integrity issues. However, the integrity-checking program is not in use. To mitigate this risk, a policy and procedure for protecting data integrity was developed. The covered entity determined this new policy and procedure will also meet Security Rule requirements. The policy requires manual and technological processes to ensure that any data, including EPHI, is not altered or destroyed in an improper manner. The policy references the information system activity review and information access management policies as supplemental policies for protecting data against improper alteration or destruction (§ 164.312(c)(1)).

[108] See Section 4.8, *HIPAA Standard: Evaluation.*
[109] See Section 4.8, *HIPAA Standard: Evaluation.*
[110] See Section 4.6, *HIPAA Standard: Security Incident Procedures.*

The procedure for maintaining data integrity required the use of the technical data integrity-checking program included in the information system. The covered entity decided the program should be run every other week or as needed. Prior to running the program the system administrator must notify users that the system will be unavailable during a certain period of time for system maintenance. During this period of down time the administrator must run system diagnostics and identify any integrity issues that if uncorrected could cause destruction of PHI. Once the issues are identified the administrator executes the integrity-checking program to fix the problem. After these steps are performed the system is restored to normal operating mode (§ 164.312(c)(2)).

Explanation:

The covered entity's decision to implement a new policy and procedures for data integrity and to use existing technical integrity measures of the information system is reasonable and appropriate given the covered entity's circumstances. 45 CFR § 164.312(c)(1) requires a covered entity to implement policies and procedures to protect electronic protected health information from improper alteration or destruction. The entity's decision to require manual and technological processes for data integrity in the policy is also reasonable and appropriate for its environment. The policy would not be reasonable and appropriate if the manual process or technical capabilities of the system did not identify integrity issues until after the EPHI was already altered or destroyed.

The covered entity's decision to implement procedures for maintaining data integrity that includes the use of a technical data integrity-checking program that is part of the information system is appropriate for its environment. The addressable implementation specification at § 164.312(c)(2) requires a covered entity to determine whether it is reasonable and appropriate to implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. The entity's decision to implement the electronic data integrity checking mechanism within the information system to corroborate the integrity of EPHI and to run the program every other week or as needed, does allow the entity to meet this addressable implementation specification. The Security Rule does not require a frequency for running the electronic mechanisms. The procedure may not be reasonable and appropriate if the technical measures do not corroborate integrity of EPHI until after it is altered or destroyed in an unauthorized manner.

4.17 Person or Entity Authentication (§ 164.312(d))[111]

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
Note: This HIPAA Standard does not include any implementation specifications.	**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. Under the HIPAA Security Rule, authentication is the corroboration that a person is the one claimed. (45 CFR § 164.304). • Authentication requires establishing the validity of a transmission source and/or verifying an individual's claim that he or she has been authorized for specific access privileges to information and information systems.	• What authentication methods are available? • What are the advantages and disadvantages of each method? • What will it cost to implement the available methods in our environment? • Do we have trained staff who can maintain the system or do we need to consider outsourcing some of the support? • Are passwords being used? • If so, are they unique by individual?
2. Evaluate Authentication Options Available	• Weigh the relative advantages and disadvantages of commonly used authentication approaches. • There are four commonly used authentication approaches available: – Something a person knows, such as a password, – Something a person has or is in possession of, such as a token (smart card, ATM card, etc.), – Some type of biometric identification a person provides, such as a fingerprint, or – A combination of two or more of the above approaches.	• What are the strengths and weaknesses of each available option? • Which can be best supported with assigned resources (budget/staffing)? • What level of authentication is appropriate based on our assessment of risk to the information/systems? • 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 Key Activity 2, above, and select appropriate authentication methods. • Implement the methods selected into your operations and activities.	• Has necessary user and support staff training been completed? • Have formal authentication policy and procedures been established and communicated? • Has necessary testing been completed to ensure that the authentication system is working as prescribed? • Do the procedures include ongoing system maintenance and updates? • Is the process implemented in such a way that it does not

[111] See also Section 4.14, *HIPAA Standard: Access Control* and Section 4.15, *HIPAA Standard: Audit Controls.*.

Key Activities	Description	Sample Questions
		compromise the authentication information (password file encryption, etc.)
Supplemental References	• NIST SP 800-14 • NIST SP 800-53 • NIST SP 800-63	

Example:

Most of EXLHCP's information systems use passwords for user authentication. After performing a recent risk analysis, the decision was made to maintain this method until a more technologically sound and cost-effective means of authentication is available. EXLHCP's Information Access Management policy requires all users to enter their user name and password to access information systems. To implement this policy the central management organization's IS department developed a procedure for establishing and managing passwords that all hospital locations have implemented. The procedure states that only authorized system administrators are able to establish user names and passwords to the system. The system administrator assigns an initial password during the access establishment process. The user receives the initial password delivered via interoffice mail. This initial password is used to log into the system. Once the user is logged in, the system forces them to change the initial password. The new password must meet the organization's password standards. The standards identify password length, use of special characters, and password change frequency. (§ 164.312(d))

Explanation:

The covered entity's decision to use passwords as the means for providing authentication for users accessing EPHI is reasonable and appropriate in its environment. 45 CFR § 164.312(d) requires covered entities to implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. The entity's decision to implement a procedure for establishing and maintaining passwords to support the Information Access Management policy is an appropriate method for managing the authentication process. The Security Rule does not require that a specific type of authentication method be used. The flexibility requirements at § 164.306(b)(1) allow covered entities to use any security measures that allow it to reasonably and appropriately implement the Security Rule standards and implementation specifications. The use of passwords for authentication is appropriate given the covered entity's circumstances, if the password can verify the identity of a user requesting access to the system as required by this standard. If the covered entity determines other technical security measures provide a more acceptable assurance of user identity and authentication, then the covered entity may want to research and consider future implementation of additional technical security measures for the information system.

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 – Chapters 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 of the EPHI by unauthorized sources during transmission (e.g., hackers, disgruntled employees, business competitors).[112]	• What measures exist to protect EPHI in transmission? • Is there an auditing process in place to verify that EPHI has been protected against unauthorized access during transmission?[113] • Are there trained staff members to monitor transmissions?
2. Develop and Implement Transmission Security Policy and Procedures	• Establish a formal (written) set of requirements for transmitting EPHI. • Identify methods of transmission that will be used to safeguard EPHI. • Identify tools and techniques that will be used to support the transmission security policy. • Implement procedures for transmitting EPHI using hardware and/or software, if needed.	• Have the requirements been discussed and agreed to by identified key personnel involved in transmitting EPHI? • Has a written policy been developed and communicated to system users?
3. Implement Integrity Controls **Implementation Specification (Addressable)**	• *Implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of.*	• What measures are planned to protect EPHI in transmission? • Is there assurance that information is not altered during transmission?
4. Implement Encryption **Implementation Specification (Addressable)**	• *Implement a mechanism to encrypt EPHI whenever deemed appropriate.*	• Is encryption reasonable and appropriate for EPHI in transmission? • Is encryption needed to effectively protect the information? • Is encryption feasible and cost-effective in this environment? • What encryption algorithms and mechanisms are available? • Does the covered entity have the appropriate staff to maintain a process for encrypting EPHI during transmission?

[112] See Section 4.7, *HIPAA Standard: Contingency Plan* and Section 4.1, *HIPAA Standard: Security Management Process.*
[113] See Section 4.1, *HIPAA Standard: Security Management Process.*

Key Activities	Description	Sample Questions:
		• Are staff members skilled in the use of encryption?
Supplemental References	• NIST SP 800-14 • NIST SP 800-42 • NIST SP 800-53 • NIST SP 800-63 • FIPS 140-2	

Example:

When the information system was implemented EXHP determined that use of the Internet or other open electronic communications networks put the entity at too much risk. Two years ago the organization modified its position due to advances in security technology and increases in the potential efficiencies to be gained from use of the Internet. EXHP decided to implement an external portal to allow access to EPHI over the Internet. Risks associated with the project were evaluated. A detailed architecture, including security architecture, was developed for the portal. The primary goal of the security architecture was to ensure that no unauthorized individual would access data, specifically electronic patient data that was transmitted over the Internet. The covered entity decided to secure the web portal using an encrypted transmission protocol, unique user authentication, and "view only" access to maintain data integrity. As part of its on-going risk analysis, the covered entity conducted a review of the security of the portal. After the review it was determined that security measures established during initial implementation met the Security Rule requirements (§§ 164.312(e)(1), (e)(2)(i) – (ii)).

Explanation:

The covered entity's decision to develop a security architecture for their web portal including technical measures to protect against unauthorized access to EPHI being transmitted over communications networks is reasonable and appropriate. 45 CFR § 164.312(e)(1) requires covered entities to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. The addressable implementation specification of this standard at § 164.312(e)(2)(i) for integrity controls requires covered entities to determine whether to implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. The other addressable implementation specification for this standard at § 164.312(e)(2)(ii) for encryption requires covered entities to determine whether to implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

When determining how to implement the requirements of the standard and the determination of whether to implement the addressable implementation specifications the entity reviewed risk analysis results and available security measures for reducing the risk of transmitting EPHI over the Web portal. The entity's decision to implement encryption of data via a secure transmission protocol and maintain integrity control of data with encryption and view only access within the application is reasonable and appropriate and allows the entity to meet the transmission security standard and associated implementation specifications.

The decision to transmit EPHI via communications networks would not be reasonable and appropriate if the technical measures chosen to protect the transmission are not able to protect the EPHI from unauthorized access during the transmission.

Organizational Requirements

4.19 Business Associate Contracts or Other Arrangements (§ 164.314(a)(1))

HIPAA Standard: *(i)The contract or other arrangement between the covered entity and its business associate required by § 164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable. (ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful—(A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.*

Key Activities	Description	Sample Questions
	Introductory References*: Security Guide for Interconnecting Information Technology Systems* (NIST SP 800-47) and *Security Considerations in the Information System Development Life Cycle* (NIST SP 800-64)	
1. Contract Must Provide that Business Associates Adequately Protect EPHI[114] **Implementation Specification (Required)**	• *Contracts between covered entities and business associates must provide that business associates will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the EPHI that the business associate creates, receives, maintains, or transmits on behalf of the covered entity.* • May consider asking the business associate to conduct a risk assessment that addresses administrative, technical, and physical risks, if reasonable and appropriate.	• Does the written agreement between the covered entity and the business associate address the applicable functions related to creating, receiving, maintaining, and transmitting EPHI that the business associate is to perform on behalf of the covered entity?
2. Contract Must Provide that Business Associate's Agents Adequately Protect EPHI **Implementation Specification (Required)**	• *Contracts between covered entities and business associates must provide that any agent, including a subcontractor, to whom the business associate provides such information agrees to implement reasonable and appropriate safeguards to protect it;*	• Does the written agreement address the issue of EPHI access by subcontractors and other agents of the business associate?
3. Contract Must Provide that Business Associates will Report Security Incidents **Implementation**	• *Contracts between covered entities and business associates must provide that business associates will report to the covered entity any security incident of which it becomes aware.*	• Is there a procedure in place for reporting of incidents by business associates? • Have key business associate staff that would be the point of contact in the

[114] Note that business associate contracts must also comply with provisions of the HIPAA Privacy Rule. See 45 CFR, *Part 164 — Security and Privacy* § 164.504(e) (*Standard: Business associate contracts*).

Key Activities	Description	Sample Questions
Specification (Required)	• Establish a reporting mechanism and a process for the business associate to use in the event of a security incident.	event of a security incident been identified?
4. Contract Must Provide that Business Associate Will Authorize Termination of the Contract if it has been Materially Breached **Implementation Specification (Required)**	• *Contracts between covered entities and business associates must provide that the business associate will authorize termination of the contract by the covered entity if the covered entity determines that the business associate has violated a material term of the contract.* • Establish in the written agreement with business associates the circumstances under which a violation of agreements relating to the security of EPHI constitutes a material breach of the contract. • Terminate the contract if: – the covered entity learns that the business associate has violated the contract or materially breached it, and – It is not possible to take reasonable steps to cure the breach or end the violation, as applicable. • If terminating the contract is not feasible, report the problem to the Secretary of HHS.	• Have standards and thresholds for termination of the contract been included in the contract?
5. Government Entities May Satisfy Business Associate Contract Requirements through Other Arrangements **Implementation Specification (Required)**	• If the covered entity and business associate are both governmental entities, consult § 164.314 (a)(2)(ii) of the Security Rule. • *If both entities are governmental entities, the covered entity is in compliance with § 164.314 (a)(1) if:* – *It executes a Memorandum of Understanding (MOU) with the business associate that contains terms that accomplish the objectives of § 164.314(a)(2)(i), or* – *Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of § 164.314(a)(2)(i).*	• Do the arrangements provide protections for EPHI equivalent to those provided by the organization's business associate contracts? • If termination of the MOU is not possible due to the nature of the relationship between the covered entity and the business associate, are other mechanisms for enforcement available, reasonable and appropriate?
6. Other Arrangements for Covered Entities and Business Associates. **Implementation Specification (Required)**	• *If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in §160.103 to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the*	• Has the covered entity made a good faith attempt to obtain satisfactory assurances that the security standards required by this section are met? • Are attempts to obtain satisfactory assurances and the reasons assurances cannot be obtained documented?

Key Activities	Description	Sample Questions
	extent necessary to comply with the legal mandate without meeting the requirements of § 164.314(a)(2)(i), provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by § 164.314(a)(2)(ii)(A), and documents the attempt and the reasons that these assurances cannot be obtained. • *The covered entity may omit from its other arrangements authorization of the termination of the contract by the covered entity, as required by § 164.314(a)(2)(i)(D), if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.*	• Does the covered entity or its business associate have statutory obligations which require removal of the authorization of termination requirement?
Supplemental References	• NIST SP 800-12 • NIST SP 800-35 • NIST SP 800-65	

Example:

As described in the previous Administrative Safeguards example, EXLHCP has already developed business associate agreement and memorandum of understanding language as part of Privacy Rule compliance. All non-government business associates with access to PHI, including EPHI, were identified, and business associate contracts were executed. In all government business associate relationships, EXLHCP decided to use a memorandum of understanding to establish terms that mirror the language of the business associate contract.

After a review of the requirements of § 164.314(a)(2)(i), the organization determined that no modifications or additional language were needed. The original agreement and memorandum of understanding (MOU) language went beyond the direct regulatory references required by the HIPAA Privacy Rule to include technology and security related issues. Although the language is not the exact language used in the Security Rule, the covered entity determined the existing agreements and MOUs contained terms that address all of the requirements including: implementation of safeguards by the business associate and their agents or contractors, reporting of security breaches and incidents, and authorization to terminate the contract if a material term is violated (§§ 164.314(a)(1), (a)(2)(i)(A) – (D) and (a)(2)(ii)(A) – (C)).

Explanation:

The covered entity's decision not to update existing business associate contracts (BAC) and memoranda of understanding (MOU) language developed for Privacy Rule compliance a permissible way of meeting the requirements of this standard, if the language addresses all applicable requirements of the Security Rule at §§ 164.314(a)(1) – (a)(2)(ii)(C). 45 CFR § 164.314(a)(1) requires the contract or other arrangement between the covered entity and its business associate required by § 164.308(b) to meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable. The entity reviewed the existing BACs and MOUs to determine if the written language addresses all requirements of § 164.314(a)(2)(i) or (a)(2)(ii). After this review, the entity determined that all language requirements of the Security Rule are addressed including: the requirement to implement safeguards by the business associate

and their agents or contractors, reporting of security breaches and incidents, and authorization to terminate the contract if a material term is violated (§§ 164.314(a)(1), (a)(2)(i)(A) – (D) and (a)(2)(ii)(A) – (C)). The covered entity's decision to maintain existing contract and other arrangement language would not be reasonable and appropriate if it determined the existing language does not provide satisfactory assurances that the business associate will maintain reasonable and appropriate safeguards and does not address the required language at §§ 164.314(a)(1) – (a)(2)(ii)(C).

4.20 Requirements for Group Health Plans (§ 164.314(b)(1))

HIPAA Standard: Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

Key Activities	Description	Sample Questions
Note: For the definition of a "group health plan," or "health plan" see 45 CFR §160.103 or Appendix B – Glossary of this document.	**Introductory Reference***: An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12)*	
1. Amend Plan Documents of Group Health Plan to Address Plan Sponsor's Security of EPHI **Implementation Specification (Required)**	• *Amend plan documents to incorporate provisions to require the plan sponsor (e.g., an entity that sponsors a health plan) to implement administrative, technical, and physical safeguards that will reasonably and appropriately protect the confidentiality, integrity, and availability of EPHI that it creates, receives, maintains, or transmits on behalf of the group health plan.*	• Does the plan sponsor fall under the exception described in the standard? • Do the plan documents require the plan sponsor to reasonably and appropriately safeguard EPHI?
2. Amend Plan Documents of Group Health Plan to Address Adequate Separation **Implementation Specification (Required)**	• *Amend plan documents to ensure that the adequate separation between the group health plan and plan sponsor required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures.*	• Do plan documents address the obligation to keep EPHI secure with respect to the plan sponsor's employees, classes of employees, or other persons who will be given access to EPHI?
3. Amend Plan Documents of Group Health Plan to Address Security of EPHI Supplied to Plan Sponsors' Agents and Subcontractors **Implementation Specification (Required)**	• *Amend plan documents to incorporate provisions to require the plan sponsor to ensure that any agent, including a subcontractor, to whom it provides EPHI agrees to implement reasonable and appropriate security measures to protect the EPHI.*	• Do the plan documents of the group health plan address the issue of subcontractors and other agents of the plan sponsor implementing reasonable and appropriate security measures?

Key Activities	Description	Sample Questions
4. Amend Plan Documents of Group Health Plans to Address Reporting of Security Incidents **Implementation Specification (Required)**	• *Amend plan documents to incorporate provisions to require the plan sponsor to report to the group health plan any security incident of which it becomes aware.* • Establish specific policy for security incident reporting.[115] • Establish a reporting mechanism and a process for the plan sponsor to use in the event of a security incident.	• Is there a procedure in place for security incident reporting? • Are procedures in place for responding to security incidents?
Supplemental References	• NIST SP 800-35 • NIST SP 800-47 • NIST SP 800-61 • NIST SP 800-64 • NIST SP 800-65	

Example:

EXHP determined this requirement does not apply to their organization. All disclosures from the group health plan to the plan sponsor are made pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508.

Explanation:

If the information the group health plan discloses to the plan sponsor is information that does not come within §164.504(f)(1)(ii) or (iii), or as authorized under §164.508, then the group health plan must address this standard and implementation specifications or not disclose the EPHI. It would be advisable for the group health plan to document this decision.

[115] See Section 4.6, *HIPAA Standard: Security Incident Procedures.*

Policies and Procedures and Documentation Requirements

4.21 Policies and Procedures (§ 164.316(a))

HIPAA Standard: *Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.*

Key Activities	Description	Sample Questions
Note: This HIPAA Standard does not include any implementation specifications.	Introductory Reference: An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12)	
1. Create and Deploy Policies and Procedures	• Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements of the HIPAA Security Rule. • Periodically evaluate written policies and procedures to verify that:[116] – Policies and procedures are sufficient to address the standards, implementation specifications and other requirements of the HIPAA Security Rule. – Policies and procedures accurately reflect the actual activities and practices exhibited by the covered entity, its staff, its systems, and its business associates.	• Are reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements of the HIPAA Security Rule in place? • Are policies and procedures reasonable and appropriate given: – the size, complexity, and capabilities of the covered entity; – the covered entity's technical infrastructure, hardware, and software security capabilities; – the costs for security measures; and – the probability and criticality of potential risks to EPHI? • Do procedures exist for periodically re-evaluating the policies and procedures, updating them as necessary?[117]

[116] See Section 4.8, *HIPAA Standard: Evaluation.*
[117] See Section 4.8, *HIPAA Standard: Evaluation.*

2. Update Documentation of Policy and Procedures	• Change policies and procedures as is reasonable and appropriate, at any time, provided that the changes are documented and implemented in accordance with the requirements of the HIPAA Security Rule.	• Should HIPAA documentation updated in response to periodic evaluations, following security incidents, and/or after acquisitions of new technology or new procedures?As policies and procedures are changed are new versions made available and are workforce members appropriately trained?[118]
Supplemental Reference	• NIST SP 800-14	

Example:

Over the past five years, EXLHCP has developed several policies and procedures establishing positions on security related issues. The entity recognized this as an important factor to ensure compliance with the Security Rule. To ensure all policies and procedures required by the Security Rule are implemented, an inventory and gap analysis were performed in conjunction with the risk analysis at all hospital locations. EXLHCP determined that all Security Rule policies and procedures requirements have been reasonably and appropriately addressed (§ 164.316(a)).

Explanation:

The covered entity's decision to perform an inventory and gap analysis as part of the risk analysis process to determine if all policies and procedures have been developed is a permissible way of determining compliance with the requirements of this standard. The gap analysis process would not be reasonable and appropriate to comply with this standard if policies and procedures were not subsequently developed and implemented to account for identified gaps between current documented policies and procedures and that which is required by the Security Rule.

[118] See Section 4.22, *HIPAA Standard: Documentation* and Section 4.5, *HIPAA Standard: Security Awareness and Training.*

4.22 Documentation (§ 164.316(b)(1))

HIPAA Standard: *(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.*

Key Activities	Description	Sample Questions
	Introductory Reference: An Introduction to Computer Security: The NIST Handbook (NIST SP 800-12)	
1. Draft, Maintain and Update Required Documentation	• Document the decisions concerning the management, operational, and technical controls selected to mitigate identified risks. • Written documentation may be incorporated into existing manuals, policies, and other documents, or may be created specifically for the purpose of demonstrating compliance with the HIPAA Security Rule.	• Are all required policies and procedures documented? • Should HIPAA Security Rule documentation be maintained by the individual responsible for HIPAA Security implementation? • Should HIPAA Security documentation updated in response to periodic evaluations, following security incidents, and/or after acquisitions of new technology or new procedures?
2. Retain Documentation for at Least Six Years **Implementation Specifications (Required)**	• *Retain required documentation of policies, procedures, actions, activities or assessments required by the HIPAA Security Rule for 6 years from the date of its creation or the date when it last was in effect, whichever is later.*	• Have documentation retention requirements under HIPAA been aligned with the organization's other data retention policies?
3. Assure that Documentation is Available to those Responsible for Implementation **Implementation Specification (Required)**	• *Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.*	• Is the location of documentation known to all staff that need to access it? • Is availability of the documentation made known as part of education, training and awareness activities?[119]
4. Update Documentation as Required **Implementation Specification (Required)**	• *Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the EPHI.*	• Is there a version control procedure that allows verification of the timeliness of policies and procedures, if reasonable and appropriate? • Is there a process for soliciting input into updates of policies and procedures from staff, if reasonable and appropriate?

Example:

[119] See Section 4.5, *HIPAA Standard: Security Awareness and Training.*

In the past, EXHP maintained all documentation in printed binders. It has been difficult for EXHP to update the documentation and maintain version control. EXHP decided to convert from paper to electronic documentation. EXHP decided that both paper and electronic documentation will be maintained for three years. After three years all documentation will be maintained electronically, except for three printed binders that will be maintained at each location as part of the Contingency Plan. This will allow users to print out documentation as needed, and save on general printing costs. An Intranet site is currently being developed to maintain all organizational documentation including policies, procedures, actions, activities and assessments. The main office will have a site for displaying and maintaining organizational policies and procedures. Each remote state office will also have a site for their documentation (§§ 164.316(b)(1)(i) – (ii)).

The new Intranet site will also allow EXHP to meet the Security Rule requirements for documentation retention and availability. Moreover, it will make the process of updating and redistributing documentation more efficient. The organization has an existing policy on establishing and maintaining all documentation relevant to operations and administrative functions. The policy requires all documentation, in written or electronic format, to be retained for seven years from the date of creation or last revision. It requires documentation to be made available to all workforce members. It also requires a yearly review of all documentation. The review identifies any updates or revisions that need to be made in a timely manner in response to environmental or operational changes. EXHP decided to edit this policy to identify the need to make updates when changes affect the security of EPHI (§§ 164.316(b)(2)(i) – (iii)).

Explanation:

The covered entity's decision to manage all documentation for all locations in electronic form via an Intranet site within the next three years may be reasonable and appropriate for this entity. 45 CFR §164.316(b)(1)(i) – (ii) requires covered entities to; (i) maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment. The entity's decision to maintain all documentation in electronic form with three printed binders per location for contingency operations is a permissible way of meeting the requirements of this standard. However, the decision to maintain all documentation in electronic format would not be reasonable and appropriate;

- If the availability and integrity of the electronic media storing the documentation is not maintained;
- If the data on the electronic media cannot be read during the 7 year retention period;
- If the Intranet system used to distribute the documentation is not available to those persons responsible for implementing the procedures; or
- If version control is not maintained for updates and revisions to documentation and critical documentation of environmental or organizational security controls are not properly recorded.

The entity's decision to maintain all documentation for seven years from the date of creation of last revision goes beyond requirements of the Security Rule but may be reasonable and appropriate for this entity. The implementation specification at §164.316(b)(2)(i) requires covered entities to retain the documentation required by paragraph (b)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later. The Security Rule allows covered entities to implement security measures that exceed requirements and still be in compliance, such as the entity's decision to follow existing policy and retain documentation for a period of seven years instead of the required six year period.

The covered entity's decision to make all documentation available to all workforce members exceeds the requirements of the Security Rule but is a permissible way of meeting the requirements of this standard. 45 CFR § 164.316(b)(2)(ii) requires covered entities to make documentation available to those persons responsible for implementing the procedures to which the documentation pertains. The entity's decision to make all documentation available to all workforce members ensures it will meet the requirements of this implementation specification.

The entity's decision to review all documentation annually and to require any updates or revisions to documentation to be performed in a timely manner in response to environmental or operational changes may be reasonable and appropriate for this entity. The implementation specification at § 164.316(b)(2)(iii) requires covered entities to review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the EPHI. The Security Rule does not identify how often the periodic reviews of documentation must be performed. The entity's decision to review documentation yearly may be reasonable and appropriate if it also allows the entity to identify more frequently updates that are needed to respond to environmental or operational changes that affect the security of EPHI.

Appendix A—References[120]

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.

FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* February 2005.

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.

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

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

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*, May 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*, February 2005.

***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, *Electronic Authentication Guide: Recommendations of the National Institute of Standards and Technology*, June 2004.

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

NIST SP 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 28, 2005.

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/hipaa2.

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* and the Centers for Medicare and Medicaid Services (CMS)).

Administrative Safeguards [45 Code of Federal Regulations (C.F.R.) Sec. 164.304]	Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.
Addressable [45 C.F.R. Sec. 164.306(d)(3)]	Describing 21 of the HIPAA Security Rule's 42 implementation specifications. To meet the addressable implementation specifications, a covered entity must– (i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information; and (ii) As applicable to the entity - (A) Implement the implementation specification if reasonable and appropriate; or (B) If implementing the implementation specification is not reasonable and appropriate—(1) Document why it would not be reasonable and appropriate to implement the implementation specification; and (2) Implement an equivalent alternative measure if reasonable and appropriate.
Affiliated Covered Entities [45 C.F.R. Sec. 164.105(b)]	Legally separate covered entities that are under common ownership or control and that have all designated themselves as a single affiliated covered entity 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).
Authentication [45 C.F.R. Sec. 164.304]	The corroboration that a person is the one claimed.
Availability [45 C.F.R. Sec. 164.304]	The property that data or information is accessible and usable upon demand by an authorized person.
Business Associate [45 C.F.R. Sec. 160.103]	(1) Except as provided in paragraph (2) of this definition, "business associate" means, with respect to a covered entity, a person who: (i) On behalf of such covered entity or of an organized health care arrangement (as defined at 45 C.F.R. Sec. 164.501) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

	(A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or (B) Any other function or activity regulated by this subchapter; or (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in Sec. 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person. (2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement. (3) A covered entity may be a business associate of another covered entity.
Certification and Accreditation (C&A) [NIST SP 800-37]	*Certification* is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. *Accreditation* is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
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 [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.** See **Computer Security Contingency.**
Controls [NIST FIPS 199]	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. See **Security Controls.**
Countermeasures [CNSS. Inst. No.4009]	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Covered Entities [45 C.F.R. Sec.160.103]	Covered entity means: (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter. (4) Medicare Prescription Drug Card Sponsors.
Electronic Protected Health Information (electronic PHI, or EPHI) [45 C.F.R. Sec.160.103]	Information that comes within paragraphs (1)(i) or (1)(ii) of the definition of protected health information (see "protected health information").
Health Care Clearinghouse [45 C.F.R. Sec.160.103]	A public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions: (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction. (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.
Health Care Provider [45 C.F.R. Sec. 160.103]	A provider of services (as defined in section 1861(u) of the Social Security Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Social Security Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.
Health Information [45 C.F.R. Sec. 160.103]	Any information, whether oral or recorded in any form or medium, that: (1) 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 (2) 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 for the provision of health care to an individual.
Health Plan [45 C.F.R. Sec.160.103]	(1) Health plan includes the following, singly or in combination: (i) A group health plan, as defined in this section. (ii) A health insurance issuer, as defined in this section. (iii) An HMO, as defined in this section. (iv) Part A or Part B of the Medicare program under title XVIII of the Social Security Act. (v) The Medicaid program under title XIX of the Social Security Act, 42 U.S.C. 1396, et seq. (vi) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Social Security Act, 42 U.S.C. 1395ss(g)(1)). (vii) An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy. (viii) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers. (ix) The health care program for active military personnel under title 10 of the United States Code. (x) The veterans health care program under 38 U.S.C. chapter 17. (xi) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) (as defined in 10 U.S.C. 1072(4)). (xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq. (xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq. (xiv) An approved State child health plan under title XXI of the Social Security Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Social Security Act, 42 U.S.C. 1397, et seq. (xv) The Medicare + Choice program under Part C of title XVIII of the Social Security Act, 42 U.S.C. 1395w-21 through 1395w-28. (xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals. (xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Social Security Act, 42 U.S.C. 300gg-91(a)(2)).

	(2) Health plan excludes: (i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and (ii) A government-funded program (other than one listed in paragraph (1)(i)-(xvi) of this definition): (A) Whose principal purpose is other than providing, or paying the cost of, health care; or (B) Whose principal activity is: (1) The direct provision of health care to persons; or (2) The making of grants to fund the direct provision of health care to persons.
Hybrid Entity [45 C.F.R. Sec.164.103]	A single legal entity: (1) That is a covered entity; (2) Whose business activities include both covered and non-covered functions; and (3) That designates health care components in accordance with paragraph § 164.105(a)(2)(iii)(C).
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. See **Potential Impact.**
Implementation Specification [45 C.F.R. Sec. 160.103]	Specific requirements or instructions for implementing a standard.
Individually Identifiable Health Information (IIHI) [45 C.F.R. Sec. 160.103]	Information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) 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 for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to

	believe the information can be used to identify the individual.
Information Security [44 U.S.C., Sec. 3542]	Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide— (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information.
Information System [45 C.F.R. Sec. 164.304]	An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.[121]
Information Technology [40 U.S.C., Sec. 1401]	(A) With respect to an executive agency, 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 by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. (B) The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (C) Notwithstanding subparagraphs (A) and (B), the term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.
Integrity [45 C.F.R. Sec. 164.304]	The property that data or information have not been altered or destroyed in an unauthorized manner.

[121] FISMA defines "information system" as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." 44 U.S.C., Sec. 3502.

Management Controls [NIST SP 800-18]	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 [NIST FIPS 199]	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. See **Security Controls.**
Medicare Prescription Drug Card Sponsors [Pub. L. 108-173]	A nongovernmental entity that offers an endorsed discount drug program under the Medicare Modernization Act. This fourth category of "covered entity" will remain in effect until the drug card program ends in 2006.
Mitigate [NIST SP 800-12]	To select and implement security controls to reduce risk to a level acceptable to management, within applicable constraints. See **Risk Mitigation**.
National Security Information [NIST SP 800-37]	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 [NIST SP 800-18]	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).

Physical Safeguards [45 C.F.R. Sec. 164.304]	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.
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.
Protected Health Information (PHI) [45 C.F.R., Sec. 160.103]	Individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii)Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as employer.
Required [45 C.F.R. Sec. 164.306(d)(2**]**	As applied to an implementation specification (see implementation specification, above], indicating an implementation specification that a covered entity must implement. All implementation specifications are either required or addressable (see "addressable," above).
Risk [NIST SP 800-30]	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 [NIST SP 800-12]	The selection and implementation of security controls to reduce risk to a level acceptable to management, within applicable constraints.
Safeguards [CNSS Inst. 4009, Adapted]	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security,

	and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Security [44 U.S.C., Sec. 3542]	Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide— (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information. See **Information Security.**
Security Controls [NIST FIPS 199]	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 [45 C.F.R., Sec. 160.103]	A rule, condition, or requirement: (1) Describing the following information for products, systems, services or practices: (i) Classification of components. (ii) Specification of materials, performance, or operations; or (iii) Delineation of procedures; or (2) With respect to the privacy of individually identifiable health information.
Technical Safeguards [45 C.F.R., Sec. 164.304]	The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.
Threat [NIST SP 800-30]	The potential for a threat source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.
Threat Source [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 [45 C.F.R., Sec. 164.304]	A person or entity with authorized access.
Vulnerability [NIST SP 800-37]	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.

BAC	Business Associate Contract
C&A	Certification and Accreditation
C.F.R.	Code of Federal Regulations
CIO	Chief Information Officer
CMS	Centers for Medicare and Medicaid Services
CNSS	Center for National Security Systems
CSD	Computer Security Division
CSRC	Computer Security Resource Center
EPHI	Electronic Protected Health Information
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
MOU	Memorandum of Understanding
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

US-CERT	United States Computer Emergency Readiness Team
U.S.	United States

Appendix D—HIPAA Security Rule/NIST Publications Crosswalk[122]

This appendix provides a matrix that crosswalks the Administrative, Technical and Physical Standards and Implementation Specifications of 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. **NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996. **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 to Information Technology Systems,* January 2004. **NIST SP 800-37,** *Guide for the Security Certification and Accreditation of Federal Information Systems,* May 2004. **NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems,* February 2005. **NIST SP 800-60,** *Guide for Mapping Types of Information and Information Systems to Security Categories,* March 2005 **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. **NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996. **NIST SP 800-26,** *Security Self-Assessment Guide for Information Technology Systems,* November 2001.

[122] 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
		NIST SP 800-53, *Recommended Security Controls for Federal Information Systems,* February 2005.
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. **NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996. **NIST SP 800-26,** *Security Self-Assessment Guide for Information Technology Systems,* November 2001. **NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems,* February 2005.
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. **NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996. **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 800-53,** *Recommended Security Controls for Federal Information Systems,* February 2005. **NIST SP 800-63,** *Electronic Authentication Guide: Recommendations of the National Institute of Standards and Technology,* June 2004.
164.308(a)(4)(ii)(A)	Isolating Health Care Clearinghouse Functions (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. **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 Model,* April 1998. **NIST SP 800-26,** *Security Self-Assessment Guide for Information Technology Systems,* November 2001. **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*, February 2005.
164.308(a)(5)(ii)(A)	Security Reminders (A):Periodic security updates.	
164.308(a)(5)(ii)(B)	Protection from Malicious Software (A): Procedures for guarding against, detecting, and reporting malicious software.	
164.308(a)(5)(ii)(C)	Log-in Monitoring (A):Procedures for monitoring log-in attempts and reporting discrepancies.	
164.308(a)(5)(ii)(D)	Password Management (A): 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. **NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996. **NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems,* February 2005. **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. **NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996. **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 800-30,** *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. **NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems,* February 2005.
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. **NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996. **NIST SP 800-26,** *Security Self-Assessment Guide for Information Technology Systems,* November 2001. **NIST SP 800-37,** *Guide for the Security Certification and Accreditation of Federal Information Systems,* April 2004. **NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems,* February 2005. **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 § 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 will appropriately safeguard the information.**	**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 800-35,** *Guide to Information Technology Security Services,* October 2003. **NIST SP 800-36,** *Guide to Selecting Information Security Products,* October 2003. **NIST SP 800-47,** *Security Guide for Interconnecting Information Technology Systems,* September 2002. **NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems,* February 2005. **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 **§** 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. **NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996. **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 800-30,** *Risk Management Guide to Information Technology Systems,* January 2004. **NIST SP 800-34,** *Contingency Planning Guide for Information Technology Systems,* June 2002. **NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems,* February 2005.
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. **NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996. **NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems*, February 2005.
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. **NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996. **NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems*, February 2005.

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. **NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996. **NIST SP 800-26,** *Security Self-Assessment Guide for Information Technology Systems,* November 2001. **NIST SP 800-34,** *Contingency Planning Guide for Information Technology Systems*, June 2002. **NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems*, February 2005.
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 Control: 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 § 164.308(a)(4).**	**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 800-26,** *Security Self-Assessment Guide for Information Technology Systems,* November 2001. **NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems*, February 2005. **NIST SP 800-56,** *Recommendation on Key Establishment Schemes*, January 2003. **NIST SP 800-57,** *Recommendation on Key Management*, January 2003. **NIST SP 800-63,** *Electronic Authentication Guide: Recommendations of the National Institute of Standards and Technology,* June 2004. **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. **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. **NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems*, February 2005.
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. **NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996. **NIST SP 800-26,** *Security Self-Assessment Guide for Information Technology Systems,* November 2001. **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 800-53,** *Recommended Security Controls for Federal Information Systems*, February 2005.
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. **NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996. **NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems*, February 2005. **NIST SP 800-63,** *Electronic Authentication Guide: Recommendations of the National Institute of Standards and Technology,* June 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. **NIST SP 800-14,** *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996. **NIST SP 800-26,** *Security Self-Assessment Guide for Information Technology Systems,* November 2001. **NIST SP 800-42,** *Guideline on Network Security Testing*, October 2003. **NIST SP 800-53,** *Recommended Security Controls for Federal Information Systems*, February 2005. **NIST SP 800-63,** *Electronic Authentication Guide: Recommendations of the National Institute of Standards and Technology,* June 2004. **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.	

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	NIST Publications
Administrative and Organizational Requirements		
164.314(a)(1)	**Business Associate Contracts or Other Arrangements: (i)The contract or other arrangement between the covered entity and its business associate required by § 164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable. (ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful—(A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.**	**NIST SP 800-12,** *An Introduction to Computer Security: The NIST Handbook*, October 1995. **NIST SP 800-35,** *Guide to Information Technology Security Services,* October 2003. **NIST SP 800-47,** *Security Guide for Interconnecting Information Technology Systems,* September 2002. **NIST SP 800-64,** *Security Considerations in the Information System Development Life Cycle,* October 2003. **NIST SP 800-65**, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005
164.314(a)(2)(i)	Business Associate Contracts (R): The contract between a covered entity and a business associate must provide that the business associate will-- (A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart; (B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; (C) Report to the covered entity any security incident of which it becomes aware; (D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.	

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	NIST Publications
164.314(a)(2)(ii)	Other Arrangements (R): When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) of this section, if-- (1) It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (a)(2)(i) of this section; or (2) Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (a)(2)(i) of this section.	
164.314(b)(1)	**Requirements for Group Health Plans: Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.**	**NIST SP 800-12,** An Introduction to Computer Security: The NIST Handbook, October 1995. **NIST SP 800-35,** Guide to Information Technology Security Services, October 2003. **NIST SP 800-47**, Security Guide for Interconnecting Information Technology Systems, September 2002. **NIST SP 800-61**, *Computer Security Incident Handling Guide,* January 2004. **NIST SP 800-64,** Security Considerations in the Information System Development Life Cycle, October 2003. **NIST SP 800-65**, Integrating Security into the Capital Planning and Investment Control Process, January 2005.
164.314(b)(2)(i)	Group Heath Plan Implementation Specification (R): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan.	
164.314(b)(2)(ii)	Group Heath Plan Implementation Specification (R): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (ii) Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures.	

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	NIST Publications
164.314(b)(2)(iii)	Group Heath Plan Implementation Specification (R): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information.	
164.314(b)(2)(iv)	Group Heath Plan Implementation Specification (R): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (iv) Report to the group health plan any security incident of which it becomes aware.	
164.316(a)	**Policies and Procedures: Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.**	**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.
164.316(b)(1)	**Documentation: (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.**	**NIST SP 800-12,** *An Introduction to Computer Security: The NIST Handbook*, October 1995.
164.316(b)(2)(i)	Time Limit (R): Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	NIST Publications
164.316(b)(2)(ii)	Availability (R): Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	
164.316(b)(2)(iii)	Updates (R): Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	

Appendix E—HIPAA Security Rule/FISMA Requirements Crosswalk

This appendix provides a crosswalk of the Administrative, Technical and Physical standards and implementation specifications of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule[123] 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[124]	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

[123] This crosswalk does not address the administrative and organizational requirements of the HIPAA Security Rule such as those described in Chapter 4. These activities are generally specific to demonstrating compliance with the HIPAA Security Rule rather than standards requiring the implementation of security controls, as is required by FISMA.

[124] 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[124]	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[124]	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[124]	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 Functions (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[124]	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[124]	Intersection
164.308(a)(5)(ii)(A)	Security Reminders (A):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): 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)	Log-in Monitoring (A): Procedures for monitoring log-in 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):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 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)? 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[124]	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[124]	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[124]	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 § 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 will 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 **§** 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[124]	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[124]	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[124]	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[124]	Intersection
Technical Safeguards			
164.312(a)(1)	**Access Control: 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 § 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[124]	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." **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[124]	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[124]	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." **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[124]	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?"	