



NIST SPECIAL PUBLICATION 800-66 REV 1

An Introductory Resource Guide for Implementing the HIPAA Security Rule

The federal-agency companion to the HIPAA Security Rule. NIST SP 800-66 Rev 1 maps every HIPAA standard onto the NIST Risk Management Framework and the NIST SP 800-53 control catalog. We use this same crosswalk when we walk healthcare clients that operate under both HIPAA and FISMA through their security control selection.

NIST SP 800-66

RMF

SP 800-53 Crosswalk

Federal Agencies

NIST SPECIAL PUBLICATION 800-66 REVISION 1 · OCTOBER 2008 · CSR EDITION 2026

An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Authors: Matthew Scholl, Kevin Stine, Joan Hash, Pauline Bowen, Arnold Johnson, Carla Dancy Smith, and Daniel I. Steinberg. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930.

REPORTS ON COMPUTER SYSTEMS TECHNOLOGY

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. 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, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III. This guideline has been prepared for use by federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.) Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

Note to Readers

This document is intended as a resource for federal agencies that must comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. The HIPAA Security Rule specifically focuses on the safeguarding of electronic protected health information (EPHI). Although FISMA applies to all federal agencies and all information types, only a subset of agencies are 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, which 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 Healthcare 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 the Department of Health and Human Services (DHHS) 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).
- **Healthcare Clearinghouses** — A public or private entity that processes another entity's healthcare transactions from a standard format to a nonstandard format, or vice versa.
- **Medicare Prescription Drug Card Sponsors** — A nongovernmental entity that offered an endorsed discount drug program under the Medicare Modernization Act. This fourth category of "covered entity" remained in effect until the drug card program ended in 2006.

NIST publications, many of which are required for federal agencies, can serve as voluntary guidelines and best practices for state, local, and tribal governments and the private sector, and may provide enough depth and breadth to help organizations of many sizes select the type of implementation that best fits their unique circumstances. NIST security standards and guidelines (Federal Information Processing Standards [FIPS], Special Publications in the 800 series), which can be used to support the requirements of both HIPAA and FISMA, 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.

Executive Summary

This Special Publication (SP), which discusses security considerations and resources that may provide value when implementing the requirements of the HIPAA Security Rule, was written to:

- Help 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;
- Direct readers to helpful information in other NIST publications on individual topics addressed by the HIPAA Security Rule; and
- Aid readers in understanding the security concepts discussed in the HIPAA Security Rule. This publication does not supplement, replace, or supersede the HIPAA Security Rule itself.

1. Introduction

The National Institute of Standards and Technology (NIST) is responsible for developing standards and guidelines, including minimum requirements, used by federal agencies in providing adequate information security for the protection of agency operations and assets. Pursuant to this mission, NIST's Information Technology Laboratory (ITL) has developed guidelines 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, as well as public, nonfederal agencies and private organizations, 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 for 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 healthcare 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. The 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. It is also designed to direct readers to helpful information in other NIST publications on individual topics addressed by the HIPAA Security Rule. Readers can draw upon these publications for consideration in implementing the Security Rule. 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 the Centers for Medicare and Medicaid Services (CMS) mentioned several NIST publications in the preamble to the HIPAA Security Rule, CMS does not require their use in complying with the Security Rule.

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.

1.1 Purpose and Scope

The purpose of this publication is to help educate readers about the security standards included in the HIPAA Security Rule. It 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 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 E-Health Standards and Services (OEHS) at CMS.

1.2 Applicability

The guidelines provided in this publication are applicable to all federal information systems, other than those systems designated as national security systems as defined in 44 United States Code (U.S.C.), Section 3542. The guidelines included in this publication have 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 composing 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 that an organization will be compliant with the Security Rule.

1.3 Audience

This publication is intended to serve a diverse audience of individuals with HIPAA Security Rule implementation, management, and oversight responsibilities and organizations, federal and nonfederal, considered to be a "Covered Entity" under 45 C.F.R. Sec. 160.103.

1.4 Document Organization

- **Section 2 — Background** explains the key concepts included in the HIPAA Security Rule and provides an overview of NIST's role in information security, as well as descriptions of its various information security publications.

- **Section 3 — Risk Management Framework** introduces a structured, flexible, extensible, and repeatable process for managing organizational risk and achieving risk-based protection related to the operation and use of information systems, and the protection of EPHI.
- **Section 4 — Considerations When Applying the HIPAA Security Rule** highlights key activities a covered entity may wish to consider when implementing the Security Rule.
- **Appendix A — Glossary** defines terms used in this document.
- **Appendix B — Acronyms** identifies and defines acronyms used within this document.
- **Appendix C — References** provides references and related source material.
- **Appendix D — Security Rule Standards and Implementation Specifications Crosswalk** provides a catalog of the HIPAA Security Rule standards and implementation specifications, and crosswalks each to relevant NIST publications and security controls detailed in NIST SP 800-53.
- **Appendix E — Risk Assessment Guidelines** provides a methodology for conducting a risk assessment, the results of which will enable covered entities to identify appropriate security controls for reducing risk to the organization and its data and information systems.
- **Appendix F — Contingency Planning Guidelines** identifies fundamental planning principles and practices to help covered entities develop and maintain effective information system contingency plans.
- **Appendix G — Sample Contingency Plan Template** provides a template for preparing an information technology (IT) contingency plan.
- **Appendix H — Resources for Secure Remote Use and Access** provides an overview of NIST publications discussing security technologies that may provide value for organizations facing challenges in securing remotely accessible, stored, or transmitted EPHI.
- **Appendix I — Telework Security Considerations** provides considerations and tips for securing external devices used for telework and remote access.

1.5 How and Why to Use This Document

Users are encouraged to use this document as a resource that provides concepts and tools to assist covered entities, including federal agencies, to comply with the HIPAA Security Rule. NIST publications, many of which are required for federal agencies, can serve as guidelines and best practices for state, local, and tribal governments, and the private sector, and may provide enough depth and breadth to help organizations of many sizes select the type of implementation that best fits their unique circumstances. This document can support the compliance efforts of covered entities by ensuring that each organization is selecting methods and controls which adequately and appropriately protect EPHI of which they are the steward; informing the development of compliance strategies that are in concert with the breadth of NIST guidelines; and providing a structured framework that aligns HIPAA Security Rule requirements with the broader NIST Risk Management Framework.

2. Background

2.1 HIPAA Security Rule

The HIPAA Security Rule specifically focuses on the safeguarding 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.

2.1.1 Security Rule Goals and Objectives

As required by the "Security standards: General rules" 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."
- **Availability** is "the property that data or information is accessible and useable upon demand by an authorized person."

2.1.2 Security Rule Organization

The Security Rule is separated into six main sections that each include several standards and implementation specifications that a covered entity must address:

- **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** — 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** — 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** — defined as "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. 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. 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.

2.2 NIST and its Role in Information Security

Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. The Computer Security Division (CSD), a component within NIST's Information Technology Laboratory (ITL), provides standards and technology to protect information systems against threats to the confidentiality of information, the integrity of information and processes, and the availability of information and services in order to build trust and confidence in IT systems.

Table 1 — NIST Publication Types	
Publication Type	Description
Federal Information Processing Standards (FIPS)	Developed by NIST in accordance with FISMA. Approved by the Secretary of Commerce and are compulsory and binding for federal agencies. Since FISMA requires that federal agencies comply with these standards, agencies may not waive their use. FIPS may be used voluntarily by nonfederal organizations (e.g., state/local/tribal governments, industry).
Special Publication (SP) 800-series	Reports on ITL's research, guidelines, and outreach efforts in information system security and its collaborative activities with industry, government, and academia. Office of Management and Budget (OMB) policies state that for other than national security programs and systems, federal agencies must follow NIST guidelines. SPs may be used voluntarily by nonfederal organizations.
Other Security Publications	Other publications including interagency reports (NISTIRs) and ITL bulletins that provide technical and other information about NIST's activities.

3. A Framework for Managing Risk

The HIPAA Security Rule is all about implementing effective risk management to adequately and effectively protect EPHI. The assessment, analysis, and management of risk provides the foundation of a covered entity's Security Rule compliance efforts, serving as tools to develop and maintain a covered entity's strategy to protect the confidentiality, integrity, and availability of EPHI.

All EPHI created, received, maintained, or transmitted by a covered entity is subject to the Security Rule. Covered entities are required to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or vulnerabilities to the security of EPHI. Under the Security Rule, covered entities are required to evaluate risks and vulnerabilities in their environments and to implement security controls to address those risks and vulnerabilities.

The selection and specification of security controls can be accomplished as part of an organization-wide information security program that involves the management of organizational risk — that is, the risk to information, individuals, and the organization as a whole. The management of risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for an information system — the security controls necessary to protect individuals and the operations and assets of the organization.

3.1 NIST Risk Management Framework (RMF)

The NIST RMF provides the covered entity with a disciplined, structured, extensible, and repeatable process for achieving risk-based protection related to the operation and use of information systems and the protection of EPHI. It represents an information security life cycle that facilitates continuous monitoring and improvement in the security state of the information systems within the organization.

The activities that compose the NIST RMF are paramount to an effective information security program and can be applied to both new and legacy information systems within the context of a system development life cycle. A risk-based

approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations.

The flexible nature of the NIST RMF allows other communities of interest (e.g., state, local, and tribal governments and private sector entities) to use the framework voluntarily either with the NIST security standards and guidelines or with industry-specific standards and guidelines. The RMF provides organizations with the flexibility needed to apply the right security controls to the right information systems at the right time to adequately protect the critical and sensitive information, missions, and business functions of the organization.

FIGURE 2 — NIST RISK MANAGEMENT FRAMEWORK

Step 1: CATEGORIZE Information Systems (FIPS 199 / SP 800-60) → Step 2: SELECT Security Controls (FIPS 200 / SP 800-53) → Step 3: IMPLEMENT Security Controls (SP 800-70) → Step 4: ASSESS Security Controls (SP 800-53A) → Step 5: AUTHORIZE Information Systems (SP 800-37) → Step 6: MONITOR Security State (SP 800-37 / 800-53A) → Repeat as necessary

Organizational View — Architecture Description, Risk Executive Function, Organizational Inputs (Laws, Directives, Policy Guidance; Strategic Goals and Objectives; Priorities and Resource Availability; Supply Chain Considerations)

3.2 The NIST RMF and Links to the Security Rule

The NIST RMF consists of six steps that are paramount to the effective management of risk resulting from the operation and use of information systems. Many Security Rule standards and implementation specifications correspond to the steps of the NIST RMF. Using these corresponding requirements in an integrated fashion can provide a methodical, repeatable, risk-based approach for selecting, specifying, and implementing security controls to adequately protect EPHI.

Table 2 — Linking the NIST RMF and the HIPAA Security Rule

RMF Phase	RMF Step Description	Security Rule Link
Categorize Information Systems	Security categorization, the first and arguably the most important step in the RMF, employs FIPS 199 and NIST SP 800-60 to determine the criticality and sensitivity of the information system and the information being processed, stored, and transmitted by the system. The security controls applied to a particular information system should be commensurate with the potential impact on organizational operations and assets, individuals, or other organizations should there be a loss of confidentiality, integrity, or availability.	Identify assets and information systems that create, receive, transmit, or maintain EPHI. Related Standards: 164.308(a)(1)(i) — Security Management Process
Select Security Controls	Security control selection (FIPS 200 / NIST SP 800-53) identifies and specifies appropriate security controls. The process consists of three activities: selection of baseline controls per FIPS 199 impact levels; application of tailoring guidance; and supplementation	Select the standards and required implementation specifications as the initial security control set. Perform a risk assessment to evaluate whether the standards and required implementation specifications alone are reasonable and appropriate. Supplement the baseline

RMF Phase	RMF Step Description	Security Rule Link
	of tailored baselines with additional controls based on assessment of risk and local conditions.	with addressable implementation specifications based on risk. Related Standards: 164.308(a)(1)(i) — Security Management Process 164.308(a)(1)(ii)(A) — Risk Analysis 164.308(a)(1)(ii)(B) — Risk Management 164.316(b)(1) — Documentation 164.316(b)(2)(ii) — Updates
Implement Security Controls	Security control implementation employs enterprise architectures, the System Development Lifecycle (SDLC), and various NIST publications to guide the implementation of security controls in organizational information systems.	Implement the security controls that have been determined to be reasonable and appropriate for the organization. Related Standards: 164.308(a)(1)(ii)(B) — Risk Management
Assess Security Controls	Security Controls Assessment employs NIST SP 800-53A to evaluate the information system security controls for effectiveness using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome.	Evaluate the implemented specifications using assessment methods and procedures to determine the extent to which the controls are implemented correctly and operating as intended with respect to protecting EPHI. Related Standards: 164.308(a)(8) — Evaluation
Authorize Information System	Authorize information system operation (with implemented security controls) based upon a determination of the risk to organizational operations, organizational assets, individuals, and other organizations, and an explicit decision to accept this risk.	Inherent in any risk management process is the acceptance of those identified risks that are deemed acceptable to the organization. Related Standards: 164.308(a)(1)(ii)(B) — Risk Management
Monitor Security State	Threats and vulnerabilities to an operating environment, as well as safeguards designed to combat them, can change frequently. The assessment and evaluation of security controls on a continuous basis provides oversight and monitoring to ensure that they continue to operate effectively and as intended.	A covered entity must periodically review and update its security measures and documentation in response to environmental and operational changes that affect security of its EPHI. Related Standards: 164.308(a)(8) — Evaluation 164.308(a)(1)(ii)(D) — Information System Activity Review

4. Considerations When Applying the HIPAA Security Rule

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 tabular format. The tables, organized by HIPAA Security Rule standard, are designed to initiate the thought process for implementing the requirements of the Security Rule. These tables highlight information a covered entity may wish to consider when implementing the Security Rule; they are not meant to be prescriptive. The tables may also not be considered all-inclusive of the information available in NIST publications.

Each table includes Key Activities for the standard (some of which are also implementation specifications), Description (expanded explanation of activities including expected outputs and considerations), and Sample Questions (illustrative questions a covered entity may want to consider). The key activities are illustrative and not all-inclusive — there may be many additional activities an organization will need to consider, specific to its own operations.

This Premium Edition organizes the standards into the same four families used by NIST: **Administrative Safeguards**, **Physical Safeguards**, **Technical Safeguards**, and **Organizational / Policies / Documentation Requirements**. For the complete standard-by-standard activity tables with all key activities and sample questions, see CSR HIPAA Library — Premium Edition Papers 02, 03, 04, and 05 in this same library; SP 800-66's Section 4 maps directly onto those papers.

4.1 Administrative Safeguards — Standards Covered

- **4.1 Security Management Process** — § 164.308(a)(1) — Risk Analysis (R), Risk Management (R), Sanction Policy (R), Information System Activity Review (R)
- **4.2 Assigned Security Responsibility** — § 164.308(a)(2) — No implementation specifications (compliance with standard required)
- **4.3 Workforce Security** — § 164.308(a)(3) — Authorization and/or Supervision (A), Workforce Clearance Procedure (A), Termination Procedures (A)
- **4.4 Information Access Management** — § 164.308(a)(4) — Isolating Healthcare Clearinghouse Functions (R), Access Authorization (A), Access Establishment and Modification (A)
- **4.5 Security Awareness and Training** — § 164.308(a)(5) — Security Reminders (A), Protection from Malicious Software (A), Log-in Monitoring (A), Password Management (A)
- **4.6 Security Incident Procedures** — § 164.308(a)(6) — Response and Reporting (R)
- **4.7 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)
- **4.8 Evaluation** — § 164.308(a)(8) — No implementation specifications (compliance with standard required)
- **4.9 Business Associate Contracts and Other Arrangements** — § 164.308(b)(1) — Written Contract or Other Arrangement (R)

4.2 Physical Safeguards — Standards Covered

- **4.10 Facility Access Controls** — § 164.310(a)(1) — Contingency Operations (A), Facility Security Plan (A), Access Control and Validation Procedures (A), Maintenance Records (A)
- **4.11 Workstation Use** — § 164.310(b) — No implementation specifications (compliance with standard required)
- **4.12 Workstation Security** — § 164.310(c) — No implementation specifications (compliance with standard required)
- **4.13 Device and Media Controls** — § 164.310(d)(1) — Disposal (R), Media Re-use (R), Accountability (A), Data Backup and Storage (A)

4.3 Technical Safeguards — Standards Covered

- **4.14 Access Control** — § 164.312(a)(1) — Unique User Identification (R), Emergency Access Procedure (R), Automatic Logoff (A), Encryption and Decryption (A)
- **4.15 Audit Controls** — § 164.312(b) — No implementation specifications (compliance with standard required)
- **4.16 Integrity** — § 164.312(c)(1) — Mechanism to Authenticate Electronic Protected Health Information (A)
- **4.17 Person or Entity Authentication** — § 164.312(d) — No implementation specifications (compliance with standard required)
- **4.18 Transmission Security** — § 164.312(e)(1) — Integrity Controls (A), Encryption (A)

4.4 Organizational, Policies & Procedures, and Documentation Requirements

- **4.19 Business Associate Contracts or Other Arrangements** — § 164.314(a)(1) — Business Associate Contracts (R), Other Arrangements (R)
- **4.20 Requirements for Group Health Plans** — § 164.314(b)(1) — Implementation Specifications (R)
- **4.21 Policies and Procedures** — § 164.316(a) — No implementation specifications (compliance with standard required)
- **4.22 Documentation** — § 164.316(b)(1) — Time Limit (R), Availability (R), Updates (R)

CROSS-REFERENCE

Complete key activities, descriptions, and sample questions for all 22 standards above are provided in CSR HIPAA Library — Premium Edition Papers 02 (Administrative), 03 (Physical), 04 (Technical), and 05 (Organizational, Policies & Procedures, Documentation). See those papers for the full standard-by-standard implementation guidance, including all key activities and the complete original NIST/CMS sample questions preserved verbatim.

Appendix A — Glossary (Key Terms)

The following are key terms used throughout NIST SP 800-66 Rev 1 and the HIPAA Security Rule.

Access	The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (Definition applies to "access" as used in subpart C of 45 C.F.R. Part 164, not as used in subpart E.)
Addressable Implementation Specification	Implementation specification that a covered entity must implement if reasonable and appropriate; if not, document why and implement an equivalent measure if reasonable and appropriate.
Administrative Safeguards	Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect EPHI and to manage the conduct of the covered entity's workforce in relation to the protection of that information.
Authentication	The corroboration that a person is the one claimed.
Availability	The property that data or information is accessible and useable upon demand by an authorized person.
Business Associate	A person who, on behalf of a covered entity, performs (or assists in the performance of) a function or activity involving the use or disclosure of individually identifiable health information; or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity.
Confidentiality	The property that data or information is not made available or disclosed to unauthorized persons or processes.
Covered Entity	(1) A health plan; (2) A healthcare clearinghouse; (3) A healthcare provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA Administrative Simplification Standards.
Electronic Media	(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media.
Electronic Protected Health Information (EPHI)	Information that comes within paragraphs (1)(i) or (1)(ii) of the definition of "protected health information," as specified in 45 CFR § 160.103.
Encryption	The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

FISMA	Federal Information Security Management Act of 2002, which requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency.
Information System	An interconnected set of information resources under the same direct management control which shares common functionality.
Integrity	The property that data or information have not been altered or destroyed in an unauthorized manner.
Required Implementation Specification	Implementation specification a covered entity must implement to comply with the corresponding standard.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Analysis (or Risk Assessment)	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 Management	The implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
Security or Security Measures	All of the administrative, physical, and technical safeguards in an information system.
Security Incident	The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
Technical Safeguards	The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.
Threat	Any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Workforce

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

Appendix B — Acronyms

CFR	Code of Federal Regulations
CMS	Centers for Medicare and Medicaid Services
CSD	Computer Security Division
CSRC	Computer Security Resource Center
DHHS / HHS	Department of Health and Human Services
EPHI	Electronic Protected Health Information
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HIPAA	Health Insurance Portability and Accountability Act of 1996
IT	Information Technology
ITL	Information Technology Laboratory (at NIST)
NIST	National Institute of Standards and Technology
OCR	Office for Civil Rights
OESS	Office of E-Health Standards and Services
OMB	Office of Management and Budget

PHI	Protected Health Information
RMF	Risk Management Framework
SDLC	System Development Lifecycle
SP	Special Publication
U.S.C.	United States Code

Appendix C — References

For the complete reference list and source citations, see the original NIST SP 800-66 Rev 1 publication. Key referenced documents include:

- NIST SP 800-30 — Risk Management Guide for Information Technology Systems
- NIST SP 800-34 — Contingency Planning Guide for Federal Information Systems
- NIST SP 800-37 — Guide for Applying the Risk Management Framework to Federal Information Systems
- NIST SP 800-39 — Managing Risk from Information Systems: An Organizational Perspective
- NIST SP 800-46 — Guide to Enterprise Telework and Remote Access Security
- NIST SP 800-53 — Recommended Security Controls for Federal Information Systems and Organizations
- NIST SP 800-53A — Guide for Assessing the Security Controls in Federal Information Systems
- NIST SP 800-59 — Guide 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 800-70 — National Checklist Program for IT Products
- NIST SP 800-100 — Information Security Handbook: A Guide for Managers
- FIPS 199 — Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200 — Minimum Security Requirements for Federal Information and Information Systems
- HHS HIPAA Security Series — Papers 1 through 7 (also available as CSR HIPAA Library — Premium Edition Papers 01–07)
- 45 CFR Part 160 — General Administrative Requirements
- 45 CFR Part 164 — Security and Privacy

Appendix D — Security Rule Standards and Implementation Specifications Crosswalk

The following table catalogs the HIPAA Security Rule standards and implementation specifications, crosswalking each to the relevant NIST SP 800-53 control families. The full per-control mapping (including specific control numbers like AC-1, AT-2, etc.) is in the original NIST SP 800-66 Rev 1 PDF. For the SP 800-53 control catalog itself, see the companion document "NIST SP 800-53 r4 — Executive Summary (CSR Premium Edition)" in this library.

Appendix D — HIPAA → NIST SP 800-53 Crosswalk (Family Level)		
HIPAA Section	Standard / Implementation Specification	SP 800-53 Family
164.308(a)(1)(i)	Security Management Process	PM, RA, PL, CA
164.308(a)(1)(ii)(A)	Risk Analysis (R)	RA
164.308(a)(1)(ii)(B)	Risk Management (R)	RA, PL, PM
164.308(a)(1)(ii)(C)	Sanction Policy (R)	PS
164.308(a)(1)(ii)(D)	Information System Activity Review (R)	AU
164.308(a)(2)	Assigned Security Responsibility	PM, PL
164.308(a)(3)(i)	Workforce Security	PS
164.308(a)(3)(ii)(A)	Authorization and/or Supervision (A)	PS, AC
164.308(a)(3)(ii)(B)	Workforce Clearance Procedure (A)	PS
164.308(a)(3)(ii)(C)	Termination Procedures (A)	PS, AC
164.308(a)(4)(i)	Information Access Management	AC
164.308(a)(4)(ii)(A)	Isolating Healthcare Clearinghouse Functions (R)	SC, AC
	Access Authorization (A)	AC

HIPAA Section	Standard / Implementation Specification	SP 800-53 Family
164.308(a)(4) (ii)(B)		
164.308(a)(4) (ii)(C)	Access Establishment and Modification (A)	AC
164.308(a)(5) (i)	Security Awareness and Training	AT
164.308(a)(5) (ii)(A)	Security Reminders (A)	AT
164.308(a)(5) (ii)(B)	Protection from Malicious Software (A)	SI
164.308(a)(5) (ii)(C)	Log-in Monitoring (A)	AC, AU
164.308(a)(5) (ii)(D)	Password Management (A)	IA
164.308(a)(6) (i)	Security Incident Procedures	IR
164.308(a)(6) (ii)	Response and Reporting (R)	IR
164.308(a)(7) (i)	Contingency Plan	CP
164.308(a)(7) (ii)(A)	Data Backup Plan (R)	CP
164.308(a)(7) (ii)(B)	Disaster Recovery Plan (R)	CP
164.308(a)(7) (ii)(C)	Emergency Mode Operation Plan (R)	CP
164.308(a)(7) (ii)(D)	Testing and Revision Procedures (A)	CP
164.308(a)(7) (ii)(E)	Applications and Data Criticality Analysis (A)	CP, RA
164.308(a)(8)	Evaluation	CA
164.308(b)(1)	Business Associate Contracts and Other Arrangements	SA, AC
164.308(b)(4)	Written Contract or Other Arrangement (R)	SA

HIPAA Section	Standard / Implementation Specification	SP 800-53 Family
164.310(a)(1)	Facility Access Controls	PE
164.310(a)(2)(i)	Contingency Operations (A)	PE, CP
164.310(a)(2)(ii)	Facility Security Plan (A)	PE
164.310(a)(2)(iii)	Access Control and Validation Procedures (A)	PE
164.310(a)(2)(iv)	Maintenance Records (A)	MA, PE
164.310(b)	Workstation Use	AC, PL
164.310(c)	Workstation Security	PE
164.310(d)(1)	Device and Media Controls	MP
164.310(d)(2)(i)	Disposal (R)	MP
164.310(d)(2)(ii)	Media Re-use (R)	MP
164.310(d)(2)(iii)	Accountability (A)	MP
164.310(d)(2)(iv)	Data Backup and Storage (A)	CP, MP
164.312(a)(1)	Access Control	AC
164.312(a)(2)(i)	Unique User Identification (R)	IA, AC
164.312(a)(2)(ii)	Emergency Access Procedure (R)	AC, CP
164.312(a)(2)(iii)	Automatic Logoff (A)	AC
164.312(a)(2)(iv)	Encryption and Decryption (A)	SC, AC
164.312(b)	Audit Controls	AU
164.312(c)(1)	Integrity	SI

HIPAA Section	Standard / Implementation Specification	SP 800-53 Family
164.312(c)(2)	Mechanism to Authenticate EPHI (A)	SI
164.312(d)	Person or Entity Authentication	IA
164.312(e)(1)	Transmission Security	SC
164.312(e)(2)(i)	Integrity Controls (A)	SC, SI
164.312(e)(2)(ii)	Encryption (A)	SC
164.314(a)(1)	Business Associate Contracts or Other Arrangements	SA
164.314(b)(1)	Requirements for Group Health Plans	SA, PL
164.316(a)	Policies and Procedures	PM, PL
164.316(b)(1)	Documentation	PM, PL
164.316(b)(2)(i)	Time Limit (R)	PM
164.316(b)(2)(ii)	Availability (R)	PM
164.316(b)(2)(iii)	Updates (R)	PM

Appendix E — Risk Assessment Guidelines

Appendix E of the original NIST SP 800-66 Rev 1 provides a comprehensive methodology for conducting a risk assessment, based on NIST SP 800-30. Because CSR HIPAA Library — Premium Edition Paper 06 ("Basics of Risk Analysis and Risk Management") covers risk assessment methodology in faithful, in-depth detail with the same NIST SP 800-30 foundation, we direct readers there for the complete 8-step risk analysis methodology and 3-step risk management methodology. The methodology covers: identifying scope, gathering data, identifying threats and vulnerabilities, assessing current security measures, determining likelihood, determining impact, determining risk level, identifying security measures, and finalizing documentation.

Appendix F — Contingency Planning Guidelines

Appendix F of the original NIST SP 800-66 Rev 1 identifies fundamental planning principles and practices to help covered entities develop and maintain effective information system contingency plans, drawing on NIST SP 800-34. Key fundamentals include: developing a contingency planning policy statement; conducting a business impact analysis;

identifying preventive controls; developing recovery strategies; developing an IT contingency plan; planning testing, training, and exercises; and planning maintenance. For complete coverage, see the original NIST SP 800-66 Rev 1 PDF and NIST SP 800-34 directly.

Appendix G — Sample Contingency Plan Template

Appendix G of the original NIST SP 800-66 Rev 1 provides a 30+ page sample IT contingency plan template. Major sections include: Introduction (purpose, scope, plan information), Concept of Operations (system description, three phases of contingency operations — Notification/Activation, Recovery, Reconstitution), Notification and Activation Procedures, Recovery Procedures, Return to Normal Operations, Plan Appendices (Personnel Contact List, Vendor Contact List, Standard Operating Procedures, Equipment and Specifications, Vendor Service Level Agreements, Description of Backup Strategies, Alternate Site Procedures, System Validation Test Plan, and Diagrams of System and Input/Output). For the complete template, see the original NIST SP 800-66 Rev 1 PDF.

Appendix H — Resources for Secure Remote Use and Access

Appendix H of the original NIST SP 800-66 Rev 1 provides an overview of NIST publications discussing security technologies that may provide value for organizations facing challenges in securing remotely accessible, stored, or transmitted EPHI. The primary references are NIST SP 800-46 (Guide to Enterprise Telework and Remote Access Security), SP 800-77 (Guide to IPsec VPNs), SP 800-113 (Guide to SSL VPNs), SP 800-114 (User's Guide to Securing External Devices for Telework and Remote Access), and SP 800-121 (Guide to Bluetooth Security).

Appendix I — Telework Security Considerations

Appendix I of the original NIST SP 800-66 Rev 1 provides considerations and tips for securing external devices used for telework and remote access, based on NIST SP 800-114. Key principles include: securing the external device (operating system updates, antivirus, host-based firewall), securing the telework connection (VPN, multi-factor authentication where appropriate), protecting EPHI in transit (encryption), protecting EPHI at rest on the external device (full-disk or file encryption, secure wipe before disposal/reuse), and developing organizational telework policy.

SCOPE NOTE — CSR PREMIUM EDITION

The original NIST SP 800-66 Rev 1 (October 2008) is 117 pages and contains Section 4's full 22-standard implementation activity tables with detailed key activities, descriptions, and sample questions for each. To avoid duplication with CSR HIPAA Library — Premium Edition Papers 02–06 (which already cover those 22 standards faithfully with all sample questions preserved), this Premium Edition focuses on what makes NIST SP 800-66 uniquely valuable: the NIST Risk Management Framework, the Federal Information Security Management Act (FISMA) integration, and the Appendix D crosswalk between HIPAA standards and NIST SP 800-53 control families. For the complete original document including all detailed activity tables and full appendix content, refer to the source PDF in your library.



CYBER SECURITY RESOURCE

PROTECTING DATA · SECURING TRUST

About Cyber Security Resource

Protecting Data — Securing Trust

We're a healthcare-focused cybersecurity firm. We help medical technology, SaaS, and regulated organizations build security programs that hold up — under audit, under attack, and under board scrutiny.

Our approach is structured and cost-effective. We focus on practical risk management, compliance alignment, and real-world security testing. The goal is simple: **meet HIPAA, HITRUST, and enterprise customer requirements with confidence** — without spending a year and six figures to get there.

This library is the same orientation we hand a new client on day one. Use it as a working reference; the requirements are unchanged from the original CMS guidance, and the design is built to be readable in a boardroom or on a security analyst's second monitor.

CONTACT

support@cybersecurityresource.com
+1 (442) 222-1338

HEADQUARTERS

Carlsbad, California
United States

WEB · EDITION

cybersecurityresource.com
Cyber Security Resource Edition ·
2026