NIST Special Publication 800
NIST SP 800-66r2

Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

A Cybersecurity Resource Guide

Jeffrey A. Marron

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-66r2

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication 800
NIST SP 800-66r2

Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

A Cybersecurity Resource Guide

Jeffrey A. Marron
Applied Cybersecurity Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-66r2

February 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority
This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the 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. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History
Approved by the NIST Editorial Review Board on 2024-01-30
Supersedes NIST SP 800-66r1 (October 2008) https://doi.org/10.6028/NIST.SP.800-66r1

How to Cite this NIST Technical Series Publication
Marron J (2024) Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-66r2. https://doi.org/10.6028/NIST.SP.800-66r2

Author ORCID iDs
Jeffrey A. Marron: 0000-0002-7871-683X

Contact Information
sp800-66-comments@nist.gov

Additional Information

Additional information about this publication is available at https://csrc.nist.gov/pubs/sp/800/66/r2/final, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

The HIPAA Security Rule focuses on safeguarding electronic protected health information (ePHI) held or maintained by regulated entities. The ePHI that a regulated entity creates, receives, maintains, or transmits must be protected against reasonably anticipated threats, hazards, and impermissible uses and/or disclosures. This publication provides practical guidance and resources that can be used by regulated entities of all sizes to safeguard ePHI and better understand the security concepts discussed in the HIPAA Security Rule.

Keywords

administrative safeguards; Health Insurance Portability and Accountability Act; implementation specification; physical safeguards; risk assessment; risk management; Security Rule; standards; technical safeguards.

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. The 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.

Document Conventions

The terms “should” and “should not” indicate that, among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited.

The terms “may” and “need not” indicate a course of action permissible within the limits of the publication.

The terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

Disclaimer

This publication offers general guidance and is provided for informational purposes. This publication should not be construed or relied upon as legal advice or guidance. This document does not modify the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, or any other federal law or regulation. The participation of other federal organizations with the National Institute of Standards and Technology (NIST) 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. 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.

Patent Disclosure Notice

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Table of Contents

List of Tables

List of Figures

Acknowledgments

The author wishes to thank Nick Heesters from the Department of Health and Human Services (HHS) Office for Civil Rights (OCR), who greatly contributed to the document's development. The author also gratefully acknowledges the many contributions from the public and private sectors during the public review process whose thoughtful and constructive comments improved the quality and usefulness of this publication.

Executive Summary

This publication aims to help educate readers about the security standards included in the Health Insurance Portability and Accountability Act (HIPAA) Security Rule [Sec. Rule], as amended by the Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act [HITECH] and the Genetic Information Nondiscrimination Act and Other Modifications to the HIPAA Rules [OMNIBUS],[1] as well as assist regulated entities[2] in their implementation of the Security Rule. It includes a brief overview of the HIPAA Security Rule, provides guidance for regulated entities on assessing and managing risks to electronic protected health information (ePHI), identifies typical activities that a regulated entity might consider implementing as part of an information security program, and lists additional resources that regulated entities may find useful when implementing the Security Rule.

The Security Rule is flexible, scalable, and technology-neutral. For that reason, there is no one single compliance approach that will work for all regulated entities. This publication presents guidance that entities can utilize in whole or in part to help improve their cybersecurity posture and assist with achieving compliance with the Security Rule.

The HIPAA Security Rule specifically focuses on safeguarding the confidentiality, integrity, and availability of ePHI. All HIPAA-regulated entities must comply with the requirements of the Security Rule. The ePHI that a regulated 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 regulated 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 U.S. Department of Health and Human Services (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).
- **Healthcare Clearinghouses** — A public or private entity that processes another entity's healthcare transactions from a standard format to a non-standard format or vice versa.
- **Business Associate** — A person or entity[3] that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of or provides services to a covered entity. A business associate is liable for their own HIPAA violations.

[1] For the remainder of this document, references to and discussions about the Security Rule will be to the Security Rule as amended by the Omnibus Rule unless otherwise specified.
[2] A "regulated entity" refers to both covered entities and business associates as defined in the Security Rule. Business associates also include business associates' subcontractors who have access to protected health information (PHI).
[3] A member of the covered entity's workforce is not a business associate. A covered healthcare provider, health plan, or healthcare clearinghouse can be a business associate of another covered entity.

The Security Rule is separated into six main sections that each include several standards that a regulated entity must meet. Many of the standards contain implementation specifications. An implementation specification is a more detailed description of the method or approach that regulated entities can use to meet a particular standard. Implementation specifications are either required or addressable. Regulated entities must comply with required implementation specifications. Regulated entities must perform an assessment to determine whether each addressable implementation specification is a reasonable and appropriate safeguard to implement in the regulated entity's environment.

The assessment, analysis, and management of risk to ePHI provide the foundation for a regulated entity's Security Rule compliance efforts and the protection of ePHI. Readers are reminded of the Security Rule's flexibility of approach. The HHS Office for Civil Rights (OCR) does not prescribe any particular risk assessment or risk management methodology. Section 3 and Sec. 4 provide background information about risk assessment and risk management processes, respectively, as well as approaches that regulated entities may choose to use in assessing and managing risk to ePHI.

Many regulated entities may benefit from more specific guidance concerning how to comply with the standards and implementation specifications of the Security Rule. To that end, Sec. 5 highlights considerations for a regulated entity when implementing the Security Rule. Key activities, descriptions, and sample questions are provided for each standard. The key activities suggest actions that are often associated with the security functions suggested by that standard. Many of these key activities are often included in a robust security program and may be useful to regulated entities. The descriptions provide expanded explanations about each of the key activities and the types of activities that a regulated entity may pursue when implementing the standard. The sample questions are a non-exhaustive list of questions that a regulated entity may ask itself to determine whether the standard has been adequately implemented.

Regulated entities may implement the Security Rule more effectively if they are shown controls catalogs and cybersecurity activities that align with each standard. To assist regulated entities, this publication includes mappings of the Security Rule's standards and implementation specifications to Cybersecurity Framework [NIST CSF] Subcategories and applicable security controls detailed in NIST Special Publication (SP) 800-53r5 (Revision 5), *Security and Privacy Controls for Information Systems and Organization*s [SP 800-53]. The mapping also lists additional NIST publications relevant to each Security Rule standard. Readers may draw upon these NIST publications and mappings for assistance in implementing the Security Rule.

Additionally, Appendix F links to a wide variety of resources (e.g., guidance, templates, tools) that regulated entities may find useful for complying with the Security Rule and improving the security posture of their organizations. For ease of use, the resources are organized by topic. Regulated entities could consult these resources when they need additional information or guidance about a particular topic.

The Security Rule is scalable and flexible by design. While the required standards and implementation specifications are the same for all regulated entities, reasonable and appropriate implementations of such standards and implementation specifications may be different for different organizations. For example, all regulated entities are required to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. An implementation of generating and examining these required audit logs that is reasonable and appropriate to reduce applicable risks to ePHI will often be vastly different for a small medical practice than for a national health plan.

1. Introduction

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule [Sec. Rule] specifically focuses on safeguarding electronic protected health information (ePHI). All HIPAA-covered entities and business associates must comply with the requirements of the Security Rule. Throughout this publication, covered entities and business associates will be referred to as *regulated entities*. Whenever the term **regulated entity** or **regulated entities** appears, it is to be understood as applying to both covered entities and business associates as defined in the Security Rule.

1.1. Purpose and Scope

NIST Special Publication (SP) 800-66 aims to help educate readers about the security standards included in the HIPAA Security Rule and assist regulated entities in their implementation of the Security Rule. It includes a brief overview of the HIPAA Security Rule, provides guidance for regulated entities in assessing and managing risk to ePHI, identifies typical activities that a regulated entity should consider when implementing an information security program, and lists additional resources that regulated entities may find useful when implementing the Security Rule.

This publication is intended to aid understanding of the HIPAA Security Rule and does not supplement, replace, modify, or supersede the Security Rule itself. Anyone seeking clarifications on the HIPAA Security Rule should contact the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR). For general HIPAA Security Rule information, visit the HHS Security Rule website.[4]

The NIST publications available as of the publication date of SP 800-66r2 (Revision 2) 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 visit the NIST Computer Security Resource Center (CSRC[5]).

1.2. Applicability

The guidance provided in this publication is applicable to all covered entities and their business associates of all sizes that store, process, or transmit ePHI. While the Security Rule requires regulated entities to safeguard ePHI, covered entities are required by the Privacy Rule[6] to safeguard all forms of protected health information (PHI). The HIPAA Privacy Rule at 164.530(c)(1) states, "A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." Essentially, this covers all oral, written, and electronic PHI (to the extent not covered by the Security Rule). Business associates maintain their own direct liability under the HIPAA Privacy, Security, and

[4] See https://www.hhs.gov/hipaa/index.html and https://www.hhs.gov/hipaa/for-professionals/security/index.html.
[5] See http://csrc.nist.gov.
[6] See https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

Breach Notification Rules (collectively, the "HIPAA Rules") with respect to their role as business associates. For example, business associates are required to comply with the Security Rule in its entirety; business associate breach notification obligations differ from that of a covered entity; and business associates are subject to liability for only certain provisions of the Privacy Rule. A summary of a business associate's direct HIPAA liability[7] is available. Federal, state, local, and tribal governments and private-sector organizations that compose the critical health infrastructure of the United States are encouraged to consider using the guidance in this publication, as appropriate.

NIST publications may be useful to any entity seeking to understand the security issues raised by the HIPAA Security Rule, regardless of that entity's size, structure, or distribution of security responsibilities. However, specific organizational missions, resources, and structures vary greatly, and entities' approaches to implementing the HIPAA Security Rule to ensure the confidentiality, integrity, and availability of ePHI may diverge significantly. SP 800-66 aims to assist all entities seeking further information on the security safeguards discussed in the HIPAA Security Rule, regardless of the 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 choose to use this publication 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. This document addresses only the security standards of the Security Rule and no other provisions adopted or raised by the HIPAA Rules, such as 45 CFR § 164.105. This document does not directly address provisions in the HIPAA Privacy, Breach Notification, or Enforcement Rules.

1.3. Document Organization

The remaining sections and appendices of this publication include the following:

- **Section 2 — HIPAA Security Rule** explains the key concepts included in the HIPAA Security Rule.
- **Section 3 — Risk Assessment Guidelines** provides a methodology for conducting a risk assessment, the results of which will enable regulated entities to identify appropriate security controls for reducing risk to ePHI.
- **Section 4 — Risk Management Guidelines** introduces a structured, flexible, extensible, and repeatable process that regulated entities may utilize to manage identified risks and achieve risk-based protection of ePHI.
- **Section 5 — Considerations When Applying the HIPAA Security Rule** highlights key activities that a regulated entity may wish to consider implementing, as well as questions that a regulated entity might ask itself when implementing the Security Rule.

[7] See https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html.

- **References** provides references and related source material.
- **Appendix A — List of Symbols, Abbreviations, and Acronyms** identifies and defines the acronyms used within this document.
- **Appendix B — Glossary** defines the terms used in this document.
- **Appendix C — Risk Assessment Tables** includes many tables referenced in Section 3, Risk Assessment Guidelines.
- **Appendix D — Security Rule Standards and Implementation Specifications Crosswalk** provides a catalog of the HIPAA Security Rule standards and implementation specifications and maps each to relevant Cybersecurity Framework [NIST CSF] Subcategories and the security controls in [SP 800-53]. It also provides a crosswalk to other relevant NIST publications that regulated entities may find useful when implementing the Security Rule.
- **Appendix E — National Online Informative References (OLIR) Program** introduces the OLIR program and how it can assist regulated entities in implementing the Security Rule.
- **Appendix F — HIPAA Security Rule Resources** provides an annotated, topical list of additional resources that regulated entities may find useful when implementing the standards and implementation specifications of the Security Rule.
- **Appendix G — Change Log** provides a list of the changes made in Revision 2.

1.4. How to Use This Document

Readers are reminded that the Security Rule is flexible, scalable, and technology-neutral. For that reason, there is no one single compliance approach that will work for all regulated entities. This publication presents guidance that entities can utilize in whole or in part to help improve their cybersecurity posture and assist with achieving compliance with the Security Rule.

Readers are encouraged to use this document as a resource for concepts and tools to assist regulated entities in complying with the HIPAA Security Rule. Risk assessment and risk management processes are foundational to a regulated entity's compliance with the Security Rule and the safeguarding of ePHI. For that reason, regulated entities may benefit from initially focusing on Sec. 3 and Sec. 4 to build fundamental risk management processes. Section 5 may be useful to regulated entities seeking activities to implement for each of the Security Rule standards or for regulated entities that want sample questions to self-evaluate their protection of ePHI. Regulated entities may also find value in the appendices that provide an annotated list of relevant resources, discussions of relevant topics, and a crosswalk to controls and practices that may help in implementing the Security Rule.

Small, regulated entities may benefit from the resources listed in Appendix F, especially the Health Industry Cybersecurity Practices (HICP) Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations. Additionally, smaller entities may find the HHS Security Risk Assessment (SRA) Tool [SRA Tool] helpful in the essential task of assessing risk to ePHI. More information about the SRA tool can be found in Sec. 3.4. Medium and large regulated entities

may find the HICP Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations (also in Appendix F) useful.

> *The Security Rule is scalable and flexible by design. While the required standards and implementation specifications are the same for all regulated entities, reasonable and appropriate implementations of such standards and implementation specifications may be different for different organizations. For example, all regulated entities are required to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. An implementation of generating and examining these required audit logs that is reasonable and appropriate to reduce applicable risks to ePHI will often be vastly different for a small medical practice than for a national health plan.*

This resource guide can support the compliance efforts of regulated entities in many ways, including:

- Ensuring that each organization is selecting security practices and controls that adequately safeguard ePHI of which they are the steward,
- Informing the development of compliance strategies that are in concert with the size and structure of the entity,[8]
- Providing guidance on best practices for developing and implementing a risk management program, and
- Creating appropriate documentation that demonstrates effective compliance with the HIPAA Security Rule.[9]

Regulated entities should consider that employing cybersecurity practices can not only help a HIPAA regulated entity comply with the Security Rule but can also assist with compliance with other federal mandates.[10] There are also business reasons to employ cyber practices, such as averting costly breach clean-up expenses or immense reputational harm due to a cyber event. With breaches amounting to hundreds of thousands to millions of dollars and the costs to secure cyber insurance doubling or more, taking steps to improve organizational cyber posture is mission-critical. Finally, there are a growing number of occurrences in which a cybersecurity

[8] Regulated entities may have competing risks (not just risk to ePHI) vying for limited organizational resources. The Security Rule preamble recognizes this and states, "This will involve establishing a balance between the information's identifiable risks and vulnerabilities, and the cost of various protective measures, and will also be dependent upon the size, complexity, and capabilities of the covered entity, as provided in § 164.306(b)."

[9] Public Law 116–321, signed into law on January 5, 2020, offers regulated entities potential mitigations of penalties and early terminations of audits if a regulated entity can demonstrate that it has had recognized security practices in place for the previous 12 months. Both the Health Industry Cybersecurity Practices (HICP) promulgated under §405(d) and the NIST Cybersecurity Framework constitute "recognized security practices" under the statute and can help organizations meet Congressional intent by implementing the guidance contained in this NIST Special Publication.

[10] These may include the Medicare Promoting Interoperability Program, which requires an annual risk assessment to avoid Medicare financial penalties, and forthcoming cyber incident reporting mandates from the Cybersecurity & Infrastructure Security Agency (CISA) as required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

incident resulted in harms to patients. Implementing and improving cybersecurity practices can help regulated entities ensure the safety of patients.

2. HIPAA Security Rule

The HIPAA Security Rule [Sec. Rule] specifically focuses on safeguarding the confidentiality, integrity, and availability of ePHI. The ePHI that a regulated 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 regulated 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 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).
- **Healthcare Clearinghouses** — A public or private entity that processes another entity's healthcare transactions from a standard format to a non-standard format or vice versa.
- **Business Associate** — A person or entity[11] that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of or provides services to a covered entity. A business associate is liable for its own HIPAA Security Rule violations.

> *Covered entities and business associates are required to obtain written satisfactory assurances from business associates that PHI will be protected. Covered entities and business associates are permitted to require more of their business associates and even include more stringent cybersecurity requirements in a business associate agreement (BAA). These requirements would need to be agreed upon by both the covered entity and the business associate.*

2.1. Security Rule Goals and Objectives

As required by the "Security standards: General rules" section of the HIPAA Security Rule, each regulated entity must:

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

[11] A member of the covered entity's workforce is not a business associate. A covered healthcare provider, health plan, or healthcare clearinghouse can be a business associate of another covered entity.

- Ensure compliance with the Security Rule by its workforce.

The Security Rule's flexibility of approach allows regulated entities to customize how they implement HIPAA's Security Rule requirements. Cybersecurity practices will vary depending on an organization's size, complexity, technical infrastructure, and hardware, software, and security capabilities.[12] In complying with this section of the Security Rule, regulated entities must be aware of the definitions provided for confidentiality, integrity, and availability, as given by § 164.304 of the Security Rule:

- **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."

2.2. Security Rule Organization

Understanding the requirements and the terminology in the HIPAA Security Rule makes it easier to see which resources might assist in Security Rule implementation and where to find more information. The Security Rule is separated into six main sections that each include several standards and implementation specifications that a regulated entity must address:[13]

1. **Security Standards: General Rules** — Includes the general requirements that all regulated entities must meet, establishes flexibility of approach, identifies standards and implementation specifications (both required and addressable), outlines decisions that a regulated entity must make regarding addressable implementation specifications, and requires the maintenance of security measures to continue reasonable and appropriate protection of ePHI
2. **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"
3. **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"

[12] For more information on the Security Rule's flexibility of approach, see § 164.306(b) of the HIPAA Security Rule (Security standards – General rules: Flexibility of approach).
[13] 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.

4. **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"
5. **Organizational Requirements** — Includes standards for business associate contracts and other arrangements between a covered entity and a business associate and between a business associate and a subcontractor, as well as requirements for group health plans
6. **Policies and Procedures and Documentation Requirements** — Requires the implementation of reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements of the Security Rule; the maintenance of written (may be electronic) documentation and/or records that include the policies, procedures, actions, activities, or assessments required by the Security Rule; and retention, availability, and update requirements related to the documentation

A regulated entity is required to comply with all of the standards of the Security Rule with respect to all of its ePHI. Many of the standards contain implementation specifications (see **Table 1**). An implementation specification is a more detailed description of the method or approach that regulated entities can use to meet a particular standard.[14] Implementation specifications are either required or addressable. However, regardless of whether a standard includes implementation specifications, regulated entities must comply with each standard.

- A **required** implementation specification is similar to a standard in that a regulated entity must comply with it.
- To meet the **addressable** implementation specifications, a regulated 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 ePHI and (ii) as applicable to the regulated entity:
    - Implement the implementation specification if reasonable and appropriate; or
    - 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 that is reasonable and appropriate.

Regulated entities are required to document these assessments and all decisions. For federal agencies, 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.

[14] 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: Implementation specifications).

Appendix D of this document provides a mapping of the HIPAA Security Rule standards and implementation specifications to Cybersecurity Framework [NIST CSF] Subcategories and the security controls detailed in [SP 800-53]. It also provides a crosswalk to other relevant NIST publications that regulated entities may find useful when implementing the Security Rule.

For general HIPAA Security Rule information, visit the HHS Security Rule website.[15]

Table 1. Security Rule standards and implementation specifications

Standard	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)	(R)
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 Function (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 Procedure (A)
		Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
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)	(R)
Workstation Security	164.310(c)	(R)
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)

[15] See https://www.hhs.gov/hipaa/index.html.

Standard	Sections	Implementation Specifications (R) = Required, (A) = Addressable
		Emergency Access Procedure (R)
		Automatic Logoff (A)
		Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A)
		Encryption (A)

3. Risk Assessment Guidance

Risk assessment and risk management processes are foundational to a regulated entity's compliance with the Security Rule [Sec. Rule] and the safeguarding of ePHI. Readers are reminded of the Security Rule's flexibility of approach. HHS OCR does not prescribe any particular risk assessment or risk management methodology. This section provides foundational information about risk assessments and an approach that regulated entities may choose to use to assess risk to ePHI. Regulated entities are free to use another risk assessment methodology[16] that provides a comprehensive assessment of risk to ePHI.

This section incorporates the risk assessment concepts and processes described in the NIST IR 8286 [IR 8286] series (specifically, IR 8286A [IR 8286A], *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*); SP 800-30r1, *Effective Use of Risk Assessments in Managing Enterprise Risk* [SP 800-30]; and SP 800-37r2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [SP 800-37]. It is intended to assist regulated entities in identifying risks to ePHI.

The purpose of a risk assessment is to identify conditions where ePHI could be used or disclosed without proper authorization, improperly modified, or made unavailable when needed. The results of the risk assessment are used to make risk management decisions on the implementation of security measures required by the Security Rule to bring risk to ePHI into an organizationally established risk tolerance range (i.e., reasonable and appropriate level) or if additional security controls are necessary.

Key Terms Defined

When talking about risk, it is important that terminology be clearly understood. This subsection defines important terms associated with risk assessment and risk management.

- *Threat events* are circumstances or events that can have a negative impact on ePHI. Threat events can be:
    - Intentional (e.g., malicious intent)
    - Unintentional (e.g., misconfigured server, data entry error)
- *Threat sources* refer to the intent and method targeted at causing harm to ePHI. Threat sources can be:
    - Natural (e.g., floods, earthquakes, storms, tornados)
    - Human (e.g., intentional, such as identity thieves, hackers, spyware authors; unintentional, such as data entry error, accidental deletions)
    - Environmental (e.g., power surges and spikes, hazardous material contamination, environmental pollution)

[16] Regulated entities may benefit from the NIST IR 8286 series of publications for more comprehensive risk assessment methodologies, including how to integrate ePHI risk assessment with Enterprise Risk Management (ERM).

- *Vulnerabilities* are flaws or weaknesses in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat event.
- *Likelihood* refers to the probability that a given threat event is capable of exploiting a given vulnerability to cause harm.
- *Impact* refers to the magnitude of harm that can be expected to result from the loss of confidentiality, integrity, and/or the availability of ePHI.
- *Risk* refers to the extent to which an entity is threatened by a potential circumstance or event. Risk is typically a function of the likelihood and impact calculations.

It can be easy to confuse some of these terms. For example, an organization may determine that it is vulnerable to damage from power surges. The threat sources that could exploit this vulnerability may include overloaded circuits or too much load on the local grid. Other threat sources (e.g., a data entry error) may be unable to exploit this vulnerability. In this example scenario, recommended security controls could range from installing uninterruptible power supply (UPS) systems, additional fuse boxes, and standby generators to rewiring the office. These additional security controls may help to mitigate the vulnerability.

3.1. HIPAA Risk Assessment Requirements

Standard 164.308(a)(1)(i), *Security Management Process*, requires regulated entities to:

> *Implement policies and procedures to prevent, detect, contain, and correct security violations.*

The Security Management Process standard includes four required implementation specifications. Two of these specifications deal directly with risk analysis[17] and risk management:

1. **Risk Analysis (R[18])** — 164.308(a)(1)(ii)(A): 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 or business associate.
2. **Risk Management (R)** — 164.308(a)(1)(ii)(B): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).

Section 3.2 provides a risk assessment methodology that regulated entities may choose to utilize in accordance with 164.308(a)(1)(ii)(A). Section 4 provides risk management best practices.

[17] In the Security Rule and throughout this document, risk analysis refers to that which is required by the Security Rule — namely, an accurate and thorough assessment of the threats and vulnerabilities to ePHI. Risk assessment refers to the process by which a regulated entity can determine the level of risk to ePHI. Section 3.2 provides a risk assessment process that regulated entities may use. Small, regulated entities may find benefit in using the HHS Security Risk Assessment (SRA) Tool.
[18] "R" indicates a required implementation specification.

3.2. How to Conduct the Risk Assessment

Risk assessments can be conducted using many different methodologies. There is no single methodology that will work for all regulated entities and all situations. The following steps represent key elements in a comprehensive risk assessment process and provide an example of the risk assessment methodology described in [IR 8286A] and [SP 800-30]. These steps should be customized to effectively identify risk for a regulated entity. The steps listed are not prescriptive in the order that they should be conducted. Some steps could be conducted simultaneously rather than sequentially.

1. **Prepare for the assessment.** Before beginning the risk assessment, the regulated entity should understand where ePHI is created, received, maintained, processed, and transmitted. Identify where ePHI is generated within the organization, where and how it enters the organization (e.g., web portals), where it moves and flows within the organization (e.g., to specific information systems), where it is stored, and where it leaves the organization. Determine whether ePHI is transmitted to external third parties, such as cloud service providers[19] or other service providers. The regulated entity can also note how access to ePHI is controlled and whether ePHI is encrypted in storage and in transit.

   The scope of a risk assessment should include both the physical boundaries of a regulated entity's location and a logical boundary that covers any devices or media that contain ePHI, including electronic networks through which ePHI is transmitted, regardless of its location. Ensure that the risk assessment scope considers teleworkers and any remote workforce, including external service providers who may have remote access to ePHI. The scope should include all removable media and portable computing devices (e.g., laptops, mobile devices) as well as the myriad of medical devices (e.g., Internet of Things [IoT] used in healthcare) that can store, process, or transmit ePHI. Modern mobile devices and installed apps may not only contain ePHI but may also pose a greater risk to ePHI due to theft or loss. In many ways, the risk assessment process will consider risks to ePHI as it enters the organization, flows within the organization, and leaves the organization.[20] Additionally, the regulated entity should consider identifying the security controls currently being used to protect ePHI.

   This preparation step is essential to ensuring that vulnerabilities and threats are correctly identified in the risk assessment process. For example, if the regulated entity does not fully identify all parties or systems to which ePHI is transmitted, it may not be possible to completely identify all relevant threats and vulnerabilities. The level of effort needed to gather the necessary information depends heavily on the scope of the assessment and the size and complexity of the regulated entity. Regulated entities may benefit from completing a business impact analysis (BIA) to evaluate, record, and monitor the criticality of organizational assets, including ePHI. The BIA can help inform

[19] Appendix F includes useful resources related to cloud services, including the OCR Guidance on HIPAA & Cloud Computing.
[20] An example consideration for regulated entities is online tracking technologies that collect and analyze information about how internet users are interacting with a regulated entity's website or mobile application. HHS provides guidance for the secure use of online tracking technologies. Regulated entities should consider whether they are hosting portals or other products that collect PHI, as well as how is that data being used, shared, and protected.

the determination of organizational risk tolerance levels, which is valuable for the risk management processes discussed in Sec. 4. Additionally, a completed BIA facilitates the completion of Step 5, "Determine the Impact of a Threat Exploiting a Vulnerability," in this proposed risk assessment process.

2. **Identify reasonably anticipated threats.** The regulated entity identifies the potential threat events and threat sources that are applicable to it and its operating environment. The list of threat events and threat sources should include reasonably anticipated and probable human and natural incidents that can negatively impact the regulated entity's ability to protect ePHI. Use the information gathered from Step 1 (i.e., the preparation step) to identify reasonably anticipated threats to ePHI. Be sure to consider threats to the confidentiality, integrity, and availability of ePHI via phishing, ransomware, or insider threat.

   Regulated entities may use various sources[21] when identifying relevant threats. Some of the resources listed in Appendix F may help regulated entities identify common threats to small, medium, and large organizations. Internet searches, vendor information, insurance data, and crime statistics are also viable sources of threat data. Regulated entities may benefit from participating in an information sharing and analysis center (ISAC) or information sharing and analysis organization (ISAO[22]) to receive threat intelligence. Ultimately, regulated entities should identify all reasonably anticipated threats to ePHI. Examples of some common threat sources are listed in **Table 2**. Regulated entities can also use **Tables 8–10** in Appendix C as resources for identifying relevant threat events and threat sources.

Table 2. Common threat sources

Type	Examples
Natural	Floods, earthquakes, tornados, landslides, avalanches, electrical storms, and other such events
Human	Events that are either enabled by or caused by human beings, such as unintentional acts (e.g., inadvertent data entry) or deliberate actions (e.g., network-based attacks, malicious software upload, unauthorized access to confidential information)
Environmental	Long-term power failure, pollution, chemicals, liquid leak

3. **Identify potential vulnerabilities and predisposing conditions.** For any of the various threats identified above to result in an impactful risk, each needs a vulnerability or predisposing condition that can be exploited. A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. A predisposing condition[23] is a condition that exists within an organization, a mission/business process, or information system that

[21] Regulated entities may benefit from [IR 8286A], specifically Section 2.2.2, when identifying threats to ePHI.
[22] See also the OCR Quarter 1 2022 Cybersecurity Newsletter.
[23] Predisposing conditions include, for example, the location of a facility in a hurricane- or flood-prone region (increasing the likelihood of exposure to hurricanes or floods) or a stand-alone information system with no external network connectivity (decreasing the likelihood of exposure to a network-based cyber attack). These types of vulnerabilities create a predisposition to threat events having adverse impacts on organizations.

contributes to (i.e., increases or decreases) the likelihood that a threat event will result in adverse impacts once initiated. The identification of vulnerabilities or predisposing conditions that a threat could exploit to cause an impact is an important component of risk assessment. While it is necessary to review threats and vulnerabilities as unique elements, they are often considered at the same time. Many organizations will consider a given loss scenario and evaluate both, such as what threat sources might initiate which threat events or what vulnerabilities or predisposing conditions those threat sources might exploit to cause an adverse impact.

The regulated entity develops a list of vulnerabilities (i.e., flaws or weaknesses) that could be exploited by potential threat sources. This list should focus on both technical and non-technical areas where ePHI can be disclosed without proper authorization, improperly modified, or made unavailable when needed. Regulated entities should use internal and external sources to identify potential vulnerabilities. Internal sources may include previous risk assessments, vulnerability scan and system security test results (e.g., penetration tests), and audit reports. External sources may include internet searches, vendor information, insurance data, and vulnerability databases, such as the National Vulnerability Database [NIST NVD]. Appendix F provides a suggested (but not all-inclusive) resource list that organizations may wish to use in vulnerability identification.

4. **Determine the likelihood that a threat will exploit a vulnerability.** The regulated entity determines the likelihood of a threat successfully exploiting a vulnerability. For each threat event/threat source identified in Step 2, consider:

    - The likelihood that the threat will occur
    - The likelihood that an occurred threat would exploit a vulnerability identified in Step 3 and result in an adverse impact

    A regulated entity might consider assigning a likelihood value (e.g., very low, low, moderate, high, or very high) to each threat/vulnerability pairing, as shown in **Table 3**. Regulated entities should feel free to use a different likelihood scale based on organizational needs.

    For example, a regulated entity may determine that the likelihood of a tornado occurring is "**Low**" (located along the leftmost column of **Table 3**) but that if it did occur, the tornado would have a "**Moderate**" likelihood (located along the top of **Table 3**) of exploiting a weakness in the facility's physical structure and resulting in an adverse impact. Using **Table 3**, the regulated entity locates the intersection of the two individual likelihood values to assign an overall likelihood of "**Low**" to this threat/vulnerability pairing. As another example, the regulated entity may determine that the likelihood of a phishing attack occurring is "**Very High**" and that the likelihood of the event exploiting a human vulnerability is "**Moderate**," resulting in an overall likelihood rating of "**High**."

Table 3. Assessment scale for overall likelihood

Likelihood of Threat Event Initiation or Occurrence	Likelihood that Threat Events Result in Adverse Impacts				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

The regulated entity could perform this likelihood assessment for each threat/vulnerability pairing. Consider that some threat events — regardless of their likelihood of occurrence — may have no vulnerability to exploit, resulting in a likelihood rating of "Very Low" or even "N/A." Conversely, some identified vulnerabilities may have no identified threat event that could exploit the vulnerability, also possibly resulting in a likelihood rating of "N/A."

5. **Determine the impact of a threat exploiting a vulnerability.** The regulated entity determines the impact that could occur to ePHI if a threat event were to exploit a vulnerability. As with likelihood determination, a regulated entity may choose to express this impact in qualitative terms (e.g., "low," "moderate," and "high") or use any other scale that the entity chooses. When selecting an impact rating, the regulated entity may consider how the threat event can affect the loss or degradation of the confidentiality, integrity, and/or availability of ePHI. Table 4 provides a brief description of each security objective (i.e., confidentiality, integrity, and availability) and the impact of it not being met. The regulated entity should select an impact rating for each identified threat/vulnerability pair.

Table 4. Security objectives and impacts

Security Objective	Impacts
Loss of Confidentiality	System and data confidentiality refers to the protection of information (e.g., ePHI) from unauthorized disclosure (i.e., the data or information is not made available or disclosed to unauthorized persons or processes). The impact of an unauthorized disclosure of ePHI can range from jeopardizing national security to disclosing data about individual persons. The unauthorized, unanticipated, or unintentional disclosure of ePHI could result in the loss of public confidence, embarrassment, legal action against the organization, and/or federal, state, and local regulatory actions.
Loss of Integrity	System and data integrity refers to the requirement that information be protected from improper modification (i.e., data or information have not been altered or destroyed in an unauthorized manner). Integrity is lost if unauthorized changes are made to the data or system by either intentional or accidental acts. If the loss of system or data integrity is not

Security Objective	Impacts
	corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. The violation of integrity may also be the first step in a successful attack against system availability or confidentiality. For all of these reasons, the loss of integrity reduces the assurance of a system.
Loss of Availability	Availability refers to the requirement that data or information be accessible and usable upon demand by an authorized person or process. If a mission-critical system is unavailable to its end users, the organization's mission may be affected. For example, the loss of system functionality and operational effectiveness may result in the loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.

Impact information can sometimes be obtained from existing organizational documentation, such as business impact and asset criticality assessments. A business impact assessment prioritizes the impact levels associated with the compromise of an organization's information assets based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets. An asset criticality assessment identifies and prioritizes the organization information assets (e.g., hardware, software, systems, services, and related technology assets) that support the organization's critical missions.

Some tangible impacts can be measured quantitatively in terms of lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other impacts cannot be measured in specific units (e.g., the loss of public confidence, the loss of credibility, or damage to an organization's interests) but can be qualitatively described (e.g., in terms of "high," "moderate," and "low" impacts). Qualitative and quantitative methods can both be used to determine the impact of a threat event exploiting a vulnerability to cause an adverse impact. Regulated entities may consult Table 5 for help with identifying potential adverse impacts and subsequently assigning an impact rating to each threat/vulnerability pair.

Table 5. Examples of adverse impacts

Type of Impact	Impact

Harm to Operations	• Inability to perform current mission or business functions
	  ○ In a sufficiently timely manner
	  ○ With sufficient confidence and/or correctness
	  ○ Within planned resource constraints
	• Inability or limited ability to restore mission or business functions in the future
	  ○ In a sufficiently timely manner
	  ○ With sufficient confidence and/or correctness
	  ○ Within planned resource constraints
	• Harms (e.g., financial costs, sanctions) due to noncompliance
	  ○ With applicable laws or regulations
	  ○ With contractual requirements or other requirements in other binding agreements (e.g., liability)
	• Direct financial costs
	• Relational harms

Type of Impact	Impact
	○ Damage to trust relationships ○ Damage to image or reputation (and, hence, future or potential trust relationships)
Harm to Assets	• Damage to or loss of physical facilities • Damage to or loss of information systems or networks • Damage to or loss of information technology or equipment • Damage to or loss of component parts or supplies • Damage to or loss of information assets • Loss of intellectual property
Harm to Individuals	• Injury or loss of life • Physical or psychological mistreatment • Identity theft • Loss of personally identifiable information • Damage to image or reputation
Harm to Other Organizations	• Harms (e.g., financial costs, sanctions) due to noncompliance ○ With applicable laws or regulations ○ With contractual requirements or other requirements in other binding agreements • Direct financial costs • Relational harms ○ Damage to trust relationships ○ Damage to reputation (and, hence, future or potential trust relationships)
Harm to the Nation	• Damage to or incapacitation of a critical infrastructure sector • Loss of government continuity of operations • Relational harms ○ Damage to trust relationships with other governments or with non-governmental entities ○ Damage to national reputation (and, hence, future or potential trust relationships) • Damage to current or future ability to achieve national objectives ○ Harm to national security

6. **Determine the level of risk.** The regulated entity assesses the level of risk to ePHI while considering the information gathered and determinations made during the previous steps. The level of risk is determined by analyzing the values assigned to the overall likelihood of threat occurrence (i.e., Step 4) and the resulting impact of threat occurrence (i.e., Step 5). **Table 6** and **Table 7** show examples of risk-level matrices that can assist in determining risk levels for each threat event/vulnerability pair. Regulated entities can use a different risk matrix that aligns with the ratings scales used for likelihood and impact in Steps 4 and 5.

Table 6. Sample risk-level matrix

Threat Likelihood	Level of Impact		
	Low	Moderate	High
High	Low	Moderate	High
Moderate	Low	Moderate	Moderate

Low	Low	Low	Low

Table 7. Detailed risk-level matrix

Threat Likelihood	Level of Impact				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

To clarify the use of the risk matrix, consider the examples presented in Step 4. For the tornado threat event, the overall likelihood was assigned a rating of "Low." However, the impact of this threat event could easily be assigned a rating of "High." Using the matrix in **Table 6**, the intersection of "**Low**" likelihood and "**High**" impact results in an overall risk rating of "**Low**." For the phishing threat example, the overall likelihood was rated "**High**." If the regulated entity determined that the impact of a phishing threat was likely to be "**Moderate**," this would result in an overall risk rating of "**Moderate**." The regulated entity should determine the level of risk for each identified threat/vulnerability pair.

7. **Document the risk assessment results.** Once the risk assessment has been completed (i.e., threat events, threat sources, and vulnerabilities identified; likelihood and impact ratings calculated; and risk levels determined), the results of the risk assessment should be documented. Regulated entities may benefit from documenting the risk assessment results in a risk register.[24] Appendix K of NIST [SP 800-30] provides a sample risk assessment report outline that may prove useful to regulated entities. Other entities may prefer to input the risk assessment results into a governance, risk, and compliance (GRC) or enterprise risk management (ERM) tool. Principally, the regulated entity should document all threat/vulnerability pairs (i.e., a scenario in which an identified threat can exploit a vulnerability) applicable to the organization, the likelihood and impact calculations, and the overall risk to ePHI for the threat/vulnerability pair. Regulated entities should consider sharing the risk assessment results with organizational leadership, whose review can be crucial to the organization's ongoing risk management.

3.3. Risk Assessment Results Affect Risk Management

The results of a risk assessment play a significant role in executing an organization's risk management strategy (presented in Sec. 4). To that end, regulated entities should not view risk assessment as a one-time, static task but as an ongoing activity. Threats change, and some

[24] OMB Circular A-11 [OMB A-11] defines a risk register as "a repository of risk information including the data understood about risks over time." The risk register provides a formal communication vehicle for sharing and coordinating cybersecurity risk activities. Regulated entities can learn more about risk registers in [IR 8286A].

identified vulnerabilities may be remediated while new vulnerabilities appear. The regulated entity may implement policies or procedures that reduce the likelihood and/or impact of a threat event. This dynamic environment requires the risk assessment to be updated on a periodic basis in order for risks to be properly identified, documented, and subsequently managed.

3.4. Risk Assessment Resources

Regulated entities may find the HHS Security Risk Assessment (SRA) Tool [SRA Tool] helpful in getting started with a risk assessment. The SRA tool was primarily developed to assist small and medium-sized regulated entities. The SRA Tool is a questionnaire that guides a regulated entity through many of the same risk assessment steps described in this section. In that sense, it is meant to be used in conjunction with the risk assessment guidance above. Regulated entities should be aware that, as a questionnaire, there are some things that the SRA tool cannot do. For example, it cannot identify technical vulnerabilities, so it — or any questionnaire tool — should be paired with a methodology that could identify technical vulnerabilities (e.g., vulnerability scanning or a vulnerability management program). Software like the SRA tool will provide output that is only as good as the information put into the tool. For that reason, regulated entities should follow an established risk assessment methodology, even when using tools for risk assessment. Regulated entities should also be aware that use of the SRA Tool or any risk assessment/management tool does not necessarily equate to compliance with the HIPAA Security Rule. Regulated entities may find additional resources in Appendix F that can assist in the risk assessment process.

4. Risk Management Guidance

The assessment and management of risk to ePHI provide the foundation for a regulated entity's Security Rule [Sec. Rule] compliance efforts. Readers are reminded of the Security Rule's flexibility of approach. HHS OCR does not prescribe any particular risk assessment or risk management methodology. This section provides background information about risk management as well as an approach from [IR 8286] that regulated entities may choose to use when managing risk to ePHI. However, regulated entities are free to use another risk management methodology[25] that effectively safeguards the confidentiality, integrity, and availability of ePHI.

All ePHI created, received, maintained, or transmitted by a regulated entity is subject to the Security Rule. Regulated entities are required to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or vulnerabilities to the confidentiality, integrity, and availability of ePHI. Risk management should be performed with regular frequency to examine past decisions, reevaluate risk likelihood and impact levels, and assess the effectiveness of past remediation efforts.

4.1. HIPAA Risk Management Requirements

Standard 164.308(a)(1)(i), *Security Management Process*, requires regulated entities to:

> *Implement policies and procedures to prevent, detect, contain, and correct security violations.*

The Security Management Process standard includes four required implementation specifications. Two of these specifications deal directly with risk analysis and risk management.

1. **Risk Analysis (R)** – 164.308(a)(1)(ii)(A): 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 or business associate.
2. **Risk Management (R)** – 164.308(a)(1)(ii)(B): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).

Section 3.2 provided a risk assessment methodology that regulated entities may choose to utilize in accordance with 164.308(a)(1)(ii)(A). This section provides risk management guidance in accordance with 164.308(a)(1)(ii)(B).

4.2. Determining Risks to ePHI in Accordance With Organizational Risk Tolerance

Regulated entities are required to assess risks and vulnerabilities in their environments and to implement security controls to address those risks and vulnerabilities. Once the risk assessment

[25] Regulated entities may benefit from the NIST IR 8286 series for more comprehensive risk management methodologies, including how to integrate ePHI risk management with Enterprise Risk Management (ERM).

has been completed and documented, the regulated entity will have a listing of applicable threat/vulnerability pairs as well as the overall risk rating of each pair to the confidentiality, integrity, and availability of ePHI.

Risk Appetite and Risk Tolerance

NIST IR 8286A presents two concepts — risk appetite and risk tolerance — that may be helpful to regulated entities in managing risk to ePHI. ***Risk appetite*** *regarding cybersecurity risks is declared at the enterprise (i.e., highest) level of the organization and provides a guidepost to the types and amount of risk that senior leaders are willing to accept in pursuit of mission objectives.* ***Risk tolerance*** *represents the specific level of performance risk deemed acceptable within the risk appetite set by senior leadership. Regulated entities may choose to express risk tolerance qualitatively (e.g., Very Low, Low, Moderate, High, or Very High) in alignment with the guidance presented in* Sec. 3.

Risk appetite and risk tolerance are related but distinct. Where risk appetite statements define the overarching risk guidance, risk tolerance statements define the specific application of that direction. This means that risk tolerance statements are always more specific than the corresponding risk appetite statements. Together, risk appetite and risk tolerance statements represent risk limits that can assist regulated entities in managing risk to ePHI.

Some threat/vulnerability pairs may indicate a moderate or high level of risk to ePHI, while others may indicate a low level of risk to ePHI. The regulated entity will need to determine what risk rating poses an unacceptable level of risk to ePHI, and any threat/vulnerability pairs that indicate a risk rating above the organizational risk tolerance will need to be addressed. If using a scale of "low," "moderate," and "high," the regulated entity may determine that any moderate or high level of risk to ePHI is unacceptable and must be remediated.

Once a regulated entity implements the standards, required implementation specifications, and addressable[26] implementation specifications in accordance with the Security Rule, the regulated entity should determine whether the risks to ePHI have been sufficiently addressed. That is, do the implemented standards and implementation specifications reduce the risk of the threat/vulnerability pairs that were deemed unacceptably high to levels that are within the organizational risk tolerance?

For example, a regulated entity's risk assessment may have identified that their ability to recover from ransomware attacks poses a high level of risk to ePHI (i.e., high likelihood rating and high impact rating). After implementing three required implementation specifications — Response and Reporting [164.308(a)(6)((ii)], Data Backup Plan [(164.308(a)(7)(ii)(A)], and Disaster Recovery Plan [164.308(a)(7)(ii)(B)] — the regulated entity reassesses that the level of risk due to ransomware attacks has been reduced to "Low." The likelihood of a ransomware attack may still be rated "High," but the three required implementation specifications have

[26] Regulated entities should consult Section 2.2 and/or the [Sec. Rule] § 164.306(d) for additional information about addressable implementation specifications and how to adequately implement them in the regulated entity's environment.

helped reduce the impact rating to "Low," resulting in an overall risk rating that is within organizational risk tolerance. Another regulated entity may have determined during a risk assessment that the loss of confidentiality of ePHI during transmission to an external party is an unacceptably high risk (i.e., outside of established risk tolerance) and that the implemented standards and implementation specifications do not reduce that risk to levels that are within organizational risk tolerance. Therefore, additional controls are needed.[27]

Ultimately, the regulated entity's risk assessment processes should inform its decisions regarding the implementation of security measures that sufficiently reduce risks to ePHI to levels within organizational risk tolerance. Each regulated entity must document[28] the security controls determined to be reasonable and appropriate, including analyses, decisions, and the rationale for decisions made to refine or adjust the security controls.

4.3. Selecting Additional Security Controls to Reduce Risk to ePHI

A regulated entity may determine that there are identified risks to ePHI that cannot be brought within established risk tolerance by any standards, required implementation specifications, or addressable implementation specifications in the Security Rule. Regulated entities should consider implementing additional security controls[29] to reduce the risk to ePHI to established risk tolerance. Appendix D provides a catalog of the HIPAA Security Rule standards and implementation specifications, each of which is mapped to relevant [NIST CSF] Subcategory outcomes and the security controls in [SP 800-53]. Regulated entities may benefit from the mapping to identify desired cybersecurity outcomes and SP 800-53 management, operational, or technical controls that can reduce the risk to ePHI to established risk tolerance.

Many organizations implement a variety of technical and non-technical controls separate from the protection of ePHI. These controls may consist of policies, processes, or technology. A thorough understanding of the entirety of security controls in place for a regulated entity may reduce the list of applicable vulnerabilities, as well as the realistic probability of a threat exploiting a vulnerability. Regulated entities should consider all technical and non-technical security controls at all places where ePHI is created, received, maintained, processed, or transmitted. Regulated entities should also determine whether these implemented or planned security measures are adequate to protect ePHI and reduce risk to ePHI to established risk tolerance. The appropriateness and adequacy of security measures may vary depending on the structure, size, and geographical dispersion of the covered entity.

For some threats and/or vulnerabilities, the regulated entity may determine that the risk to ePHI cannot be brought within established risk tolerance through any standards, implementation specifications, or additional security controls. In this case, the regulated entity's leadership may choose to revisit the established risk tolerance. The resulting

[27] See Sec. 4.3 for additional discussion.
[28] Regulated entities should consider documenting these decisions in the risk register or wherever the risk assessment results were documented. See Sec. 4.4.
[29] A cost-benefit analysis should be conducted for proposed recommended controls to demonstrate that the costs of implementing the controls can be justified by a reduction in the level of risk. In addition to cost, organizations should consider the operational impact and feasibility of introducing the recommended security controls into the operating environment.

discussions present an opportunity for leadership to determine the best course of action to refine risk acceptance and tolerance in light of mission objectives (e.g., through a risk exception process, an adjustment to the risk tolerance statement, or increased security requirements). However, if an unacceptable level of risk to ePHI cannot be adequately treated in a cost-effective manner, that risk should be avoided. Such a condition may require significantly redesigning relevant systems or processes that handle ePHI.

4.4. Documenting Risk Management Activities

As with the risk assessment, risk management activities should be documented. The regulated entity may build on the documentation developed during the risk assessment by indicating how threat/vulnerability pairs with risk levels above established risk tolerance are mitigated or avoided. Some regulated entities may choose to document their risk management activities through a risk register that records assessment findings, remediation plans, timelines, responsible parties, and other relevant information. Other regulated entities may choose to utilize free or commercially available tools to document their risk management activities. The documentation and retention of risk assessment and risk management activities may be important for future risk management efforts.

5. Considerations When Implementing the HIPAA Security Rule

This section presents security measures that are relevant to each standard of the Security Rule. Each standard is presented in a consistent tabular format. The following tables, organized by HIPAA Security Rule [Sec. Rule] standard, are designed to initiate the thought process for regulated entities to implement the requirements of the Security Rule. These tables highlight considerations for a regulated entity when implementing the Security Rule. They are not meant to be prescriptive and should not be considered comprehensive for all considerations when implementing the Security Rule.

In addition to the HIPAA Security Rule standard name and description, each table includes the following information:

- **Key Activities** — The Key Activities column lists actions that are often associated with the security functions suggested by each HIPAA Security Rule standard. Some of these key activities are also the implementation specifications for that standard. Each key activity that is also an implementation specification has been identified as such in the table (in italics in the Description section of the table) along with a note as to whether the implementation specification is required or addressable.

  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 requirements of the Security Rule. However, many of these activities are often included in a robust security process and may be useful to regulated entities. These activities may also normally be performed as part of one or more of the standard's implementation specifications. For clarity, these activities are listed as separate key activities with a footnote explaining any relationship to associated implementation specifications.

  The tables address all HIPAA Security Rule standards and all associated implementation specifications, both required and addressable. Seven of the standards include all of the necessary instructions for implementation and have no associated implementation specifications. In these instances, the standards themselves also serve as the implementation specification. 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.

  The listed key activities are illustrative and not all-inclusive. There may be additional activities that an organization will need to consider that are not included in the key activities of the tables. Each regulated entity will need to identify which activities beyond those listed in the tables are necessary and appropriate in its environment, implement those activities, and document them.

  The tables 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, readers may consult the crosswalk presented in Appendix D. For each Security Rule

standard, the crosswalk lists one or more relevant NIST publications that could provide more context or information.

- **Description** — The Description column in each table includes an expanded explanation about the key activities and the types of activities that a regulated entity may pursue when implementing a standard . These explanations are designed to help get an entity started in addressing the HIPAA Security Rule. The first description bullet of each key activity that is also an implementation specification is in italics. When a relationship exists between description bullets and other Security Rule standards or implementation specifications, it is indicated in an accompanying footnote.
- **Sample Questions** — This column includes questions that a regulated entity may ask itself to determine whether the standard has been adequately implemented. These sample questions are not exhaustive but are representative of the questions that a regulated entity may find helpful when implementing the Security Rule standards and implementation specifications. Affirmative answers to these questions do not necessarily imply that an entity is meeting all of the requirements of the HIPAA Security Rule standards. Negative answers to these questions should prompt the regulated entity to consider whether it needs to take further action to comply with the standards. Organizations with existing information security programs may have already considered many of the sample questions. The questions that an organization asks in implementing the Security Rule should be tailored to fit the unique circumstances of each entity.

This document does not discuss Section 164.105 of the HIPAA Security Rule, *Organizational Requirements*, in detail as it does not set out general security principles. HIPAA-regulated entities are encouraged to review this section of the HIPAA Security Rule in full and seek further guidance if needed.

Readers are reminded of the Security Rule's flexibility of approach. The following key activities, descriptions, and sample questions are meant to be informative, not prescriptive. This flexibility allows regulated entities to customize how they implement HIPAA's Security Rule requirements. Regulated entities should customize the key activities, descriptions, and sample questions to best fit their organization.

Each regulated entity (i.e., covered entity or business associate) is responsible for its own Security Rule compliance and violations and should review the following key activities, descriptions, and sample questions through the lens of its own organization.

5.1. Administrative Safeguards

5.1.1. Security Management Process (§ 164.308(a)(1))

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

Table 8. Key activities, descriptions, and sample questions for the Security Management Process standard

Key Activities	Description	Sample Questions
1. **Identify All ePHI and Relevant Information Systems**	• Identify where ePHI is generated within the organization, where it enters the organization, where it moves within the organization, where it is stored, and where it leaves the organization. • Identify all systems[30] that house ePHI. Be sure to identify mobile devices, medical equipment, and IoT devices that store, process, or transmit ePHI. • Include all hardware and software that are used to collect, store, process, or transmit ePHI. • Analyze business functions and verify the ownership and control of information system elements as necessary. • Consider the impact of a merger or acquisition on risks to ePHI. During a merger or acquisition, new data pathways may be introduced that lead to ePHI being stored, processed, or transmitted in previously unanticipated places.	• Has all ePHI generated, stored, processed, and transmitted within the organization been identified? • Are all hardware and software for which the organization is responsible periodically inventoried? • Is the hardware and software inventory updated on a regular basis? • Have hardware and software that maintains or transmits ePHI been identified? Does this inventory include removable media and remote access devices? • Is the current configuration of organizational systems documented, including connections to other systems? • Has a BIA been performed?
2. **Conduct Risk Assessment**[31] [32] **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 or business associate.*	• 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 United States Computer Emergency Readiness Team (US-CERT), virus alerts, and/or vendors?

[30] Regulated entities may obtain this information from an organizational business impact assessment (BIA) that has been previously completed. Alternatively, regulated entities can use the information gathered in this activity to create a BIA. See the NIST IR [8286] series of documents for more information.
[31] See Sec. 3, *Risk Assessment Guidance*, and Appendix F.
[32] The risks that must be assessed are the risks of noncompliance with the requirements of Section 164.306(a) (General Rules) of the HIPAA Security Rule.

Key Activities	Description	Sample Questions
		• What are the human, natural, and environmental threats to systems that contain, store, process, or transmit ePHI? • What are the current and planned controls? • Have likelihood and impact been determined for relevant threats and vulnerabilities? • Have risk ratings been determined for relevant threats and vulnerabilities? • Is the facility located in a region prone to any natural disasters, such as earthquakes, floods, or fires? • Has responsibility been assigned to check all hardware and software — including hardware and software used for remote access — 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**[33] **Implementation Specification (Required)**	• *Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).* • Risk management should be performed with regular frequency to examine past decisions, reevaluate risk likelihood and impact levels, and assess the effectiveness of past remediation efforts • Create a Risk Management policy and program[34] that outlines organizational risk appetite and risk tolerance, personnel duties, responsible parties, the frequency of risk management, and required documentation. • A risk management methodology is included in Sec. 4 of this document. • Risk management resources are also included in Appendix F.	• Is executive leadership and/or management involved in risk management decisions? • Has a risk management program been created with related policies? • Does the regulated entity need to engage other resources (e.g., external expertise) to assist in risk management? • 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 regulated entity used the results of risk assessment and risk management processes to guide the selection and implementation of appropriate controls to protect ePHI?

[33] See Section 164.306 of the HIPAA Security Rule.
[34] See NIST IR [8286], which describes a cybersecurity risk management program in the context of enterprise risk management.

Key Activities	Description	Sample Questions
		• Has the regulated entity protected against all reasonably anticipated threats or hazards to the security and integrity of ePHI? • Has the regulated entity assured compliance with all policies and procedures by its workforce?

4. **Acquire Information Technology (IT) Systems and Services**[35] [36]	• Regulated entities should consider how cloud services and other third-party IT system and service offerings can both assist regulated entities in protecting ePHI while also potentially introducing new risks to ePHI.
	• Although the HIPAA Security Rule does not require purchasing any particular technology, adequately protecting information may require additional hardware, software, or services. 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; and
	  ○ Other requirements, such as resources available for operation, maintenance, and training.
		• Will new security controls work with the existing IT architecture?
		• Have the security requirements of the organization been compared to 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 been developed?[37]

5. **Create and Deploy Policies and Procedures**[38] [39]	• 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.[40]	• Has the regulated entity documented an organizational risk assessment/management policy that outlines the duties, responsible parties, frequency, and required documentation of the risk management program? • Are policies and procedures in place for security? • Is there a formal (documented) system security plan? • Is there a formal contingency plan?[41]

[35] See Section 164.306(b) of the HIPAA Security Rule.
[36] See Key Activity 5.1.1.3, *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.
[37] See Sec. 5.1.5, *HIPAA Standard: Security Awareness and Training*.
[38] See Sec. 5.5.1, *HIPAA Standard: Policies and Procedures.*
[39] See Key Activity 5.1.1.3, *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.
[40] See Sec. 5.5.1, *HIPAA Standard: Policies and Procedures*, and Sec. 5.5.2, *HIPAA Standard: Documentation.*
[41] See Sec. 5.1.7, *HIPAA Standard: Contingency Plan.*

Key Activities	Description	Sample Questions
	• Create procedures to be followed to accomplish particular security-related tasks. • Establish a frequency for reviewing policy and procedures.	• 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**[42] **Implementation Specification (Required)**	• *Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.* • 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.	• Does the regulated entity have existing sanction policies and procedures to meet the requirements of this implementation specification? If not, can existing sanction policies be modified to include language related to violations of these policies and procedures? • Is there a formal process in place to address system misuse, abuse, and fraudulent activity? • Have workforce members 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 workforce members 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.* • Implement regular reviews of information system activity and consider ways to automate the review for the protection of ePHI.	• Is there a policy that establishes what reviews will be conducted? • Are there corresponding procedures that describe the specifics of the reviews? • Who is responsible for the overall process and results?[43] • How often will reviews take place? • How often will review results be analyzed? • Has the regulated entity considered all available capabilities to automate the reviews? • Where will audit information reside (e.g., separate server)? Will it be stored external to the organization (e.g., cloud service provider)?

[42] See Section 164.306 of the HIPAA Security Rule.
[43] See Sec. 5.1.2, *HIPAA Standard: Assigned Security Responsibility*.

Key Activities	Description	Sample Questions
8. **Develop Appropriate Standard Operating Procedures**[44]	• 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 and their reviews be documented and maintained?
9. **Implement the Information System Activity Review and Audit Process**[45]	• Activate the necessary review process. • Begin auditing and logging activity.	• What mechanisms will be implemented to assess the effectiveness of the review process (measures)? • What is the plan to revise the review process when needed?

[44] See Key Activity 5.1.1.7, *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.
[45] See Key Activity 5.1.1.7, *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.

5.1.2. 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 covered entity or business associate.*

Table 9. Key activities, descriptions, and sample questions for the Assigned Security Responsibility standard

Key Activities	Description	Sample Questions

1. **Select a Security Official to be Assigned Responsibility for HIPAA Security**	• Identify the individual who has final responsibility for security.[46]
	• Select an individual who is able to assess effective security 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?
		  ○ Is responsible for conducting risk management?
		  ○ Handles the results of periodic security evaluations and continuous monitoring?
		  ○ Directs IT security purchasing and investment?
		  ○ Ensures that security concerns have been addressed in system implementation?
		• Does the security official have adequate access and communications with senior officials in the organization, such as executives, chief information officers, chief compliance officers, and in-house counsel?
		• Who in the organization is authorized to accept risks from systems on behalf of the organization?

2. **Assign and Document the Individual's Responsibility**	• Document the assignment to one individual's responsibilities in a job description.[47] • 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?[48]

[46] While the security officer may enlist help from data governance or security management teams, the Security Rule states that final responsibility must be assigned to one individual.
[47] See Sec. 5.5.2, *Standard: Documentation*.
[48] See Sec. 5.1.5, *Security Awareness and Training*, and Sec. 5.1.6, *Security Incident Procedures.*

5.1.3. 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.*

Table 10. Key activities, descriptions, and sample questions for the Workforce Security standard

Key Activities	Description	Sample Questions
1. **Implement Policies and 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**[49]	• 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.[50]	• Are there written job descriptions that are correlated with appropriate levels of access to ePHI? • Are these job descriptions reviewed and updated on a regular basis? • Have workforce members been provided copies of their job descriptions and informed of the access granted to them, as well as the conditions by which this access can be used?
3. **Establish Criteria and Procedures for Hiring and Assigning Tasks**[51]	• Ensure that workforce 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.	• Have 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?

[49] See Key Activity 5.1.3.1, *Implement Policies and 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.
[50] See Sec. 5.5.2, *HIPAA Standard: Documentation.*
[51] See Key Activity 5.1.3.1, *Implement Policies and 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
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 where access is provided or terminated.	• 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? • Are there procedures for determining that the appropriate workforce members have access to the necessary information? • Do procedures exist for obtaining appropriate sign-offs to grant or terminate access to ePHI? • Have clearance and supervision procedures been developed for non-US based workforce members that are applicable to their location?
5. **Establish Termination Procedures** **Implementation Specification (Addressable)**	• *Implement procedures for terminating access to ePHI when the employment of or other arrangement with 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 (e.g., identification badges, keys, access cards) when employment ends. • Deactivate computer access accounts[52] (e.g., disable user IDs and passwords) and facility access (e.g., change facility security codes/PINs).	• Are there separate procedures for voluntary termination (e.g., retirement, promotion, transfer, change of employment) versus involuntary termination (e.g., termination for cause, reduction in force, involuntary transfer, criminal or disciplinary actions), if reasonable and appropriate? • Is there a standard checklist for all action items that should be completed when a workforce member leaves (e.g., return of all access devices, deactivation of logon accounts [including remote access], and delivery of any needed data solely under the workforce member's control)? • Do other organizations need to be notified to deactivate accounts that the workforce member had access to in the performance of their employment duties?

[52] See Sec. 5.3.1, *HIPAA Standard: Access Control*.

5.1.4. Information Access Management (§ 164.308(a)(4))[53]

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.*

Table 11. Key activities, descriptions, and sample questions for the Information Access Management standard

Key Activities	Description	Sample Questions
1. **Isolate Healthcare Clearinghouse Functions**[54] **Implementation Specification (Required)**	• *If a healthcare 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 whether a component of the regulated entity constitutes a healthcare clearinghouse under the HIPAA Security Rule. • If no clearinghouse functions exist, document this finding. If a clearinghouse exists within the organization, implement procedures for access that are consistent with the HIPAA Privacy Rule.	• If healthcare clearinghouse functions are performed, are policies and procedures implemented to protect ePHI from the other functions of the larger organization? • Does the healthcare 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, such as through access to a workstation, transaction, program, process, or other mechanism.* • Decide and document procedures for how access to ePHI will be granted to workforce members within the organization. • Select the basis for restricting access to ePHI. • Select an access control method (e.g., identity-based, role-based, or other reasonable and appropriate means of access.) • Decide and document how access to ePHI will be granted for privileged functions.	• Have appropriate authorization and clearance procedures, as specified in Workforce Security (§ 164.308(a)(3)), been performed prior to granting access? • Do the organization's systems have the capacity to set access controls?[55] • Are there documented job descriptions that accurately reflect assigned duties and responsibilities and enforce segregation of duties?[56] • Has the organization documented procedures that specify how authorized personnel will be granted access to ePHI? • Does the organization grant remote access to ePHI?

[53] See Sec. 5.2.1, *HIPAA Standard: Facility Access Controls*, and Sec. 5.3.1, *HIPAA Standard: Access Control.*
[54] 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.
[55] See Sec. 5.3.1, *HIPAA Standard: Access Control.*
[56] See Sec. 5.1.3, *HIPAA Standard: Workforce Security.*

Key Activities	Description	Sample Questions
	• Ensure that there is a list of personnel with authority to approve user requests to access ePHI and systems with ePHI. • Identify authorized users with access to ePHI, including data owners and data custodians. • Consider whether multiple access control methods are needed to protect ePHI according to the results of the risk assessment. • Determine whether 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).	• What methods of access control are used (e.g., identity-based, role-based, location-based, or a combination) to protect ePHI? • Are there additional access control requirements for users who will be accessing privileged functions? • Have organizational personnel been explicitly authorized to approve user requests to access ePHI and/or systems with ePHI?
3. **Implement Policies and Procedures for Access Establishment and Modification** **Implementation Specification (Addressable)**	• *Implement policies and procedures that – based on the covered entity or business associate's access authorization policies – establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.* • Establish standards for granting access to ePHI. • Provide formal authorization from the appropriate authority before granting access to ePHI. • Regularly review personnel access to ePHI to ensure that access is still authorized and needed • Modify personnel access to ePHI, as needed, based on review activities.	• Are duties separated such that only the minimum necessary ePHI is made available to each workforce member based on their job requirements? • Are access decisions justified, approved, logged, and retained? • Is personnel access to ePHI regularly reviewed to ensure that access is still authorized and needed? • Are activities that review access to ePHI logged and retained, including decisions that arise from review activities? • Are decisions related to the establishment and modification of workforce member authorization to access ePHI documented?
4. **Evaluate Existing Security Measures Related to Access Controls**[57]	• Evaluate the security features of access controls that are already in place or those of any planned for implementation, as appropriate. • Determine whether these security features involve alignment with other existing management, operational, and technical controls, such as policy standards, personnel procedures, the maintenance and review of audit trails,	• Are there policies and procedures related to the security of access controls?[58] If so, are they updated regularly? • Are authentication mechanisms used to verify the identity of those accessing systems protected from inappropriate manipulation?[59] • Does management regularly review the list of access authorizations, including remote access authorizations, to

[57] See Key Activity 5.1.4.3, *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.
[58] See Sec. 5.5.2, *HIPAA Section: Documentation.*
[59] See Sec. 5.3.4, *HIPAA Standard: Person or Entity Authentication.*

Key Activities	Description	Sample Questions
	the identification and authentication of users, and physical access controls.	verify that the list is accurate and has not been inappropriately altered?[60]

[60] See Sec. 5.1.3, *HIPAA Standard: Workforce Security*.

5.1.5. Security Awareness and Training (§ 164.308(a)(5))[61]

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

Table 12. Key activities, descriptions, and sample questions for the Security Awareness and Training standard

Key Activities	Description	Sample Questions
1. **Conduct a Training Needs Assessment**	• Determine the training needs of the organization. • Interview and involve key personnel in assessing security training needs. • Use feedback and analysis of past events to help determine training needs. • Review organizational behavior issues, past incidents, and/or breaches to determine what training is missing or needs reinforcement, improvement, or periodic reminders.	• What awareness, training, and education programs are needed? Which are required? • Is the organization monitoring current threats to determine possible areas of training needs? • Are there current, relevant threats (e.g., phishing, ransomware) about which personnel need training? • Do workforce members need training on any particular organization devices (e.g., IoT devices) or technology that pose a risk to ePHI? • 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 in terms of content and audience?
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. • Set organizational expectations for protecting ePHI. • In the security awareness and training program, outline the program's scope, goals, target audiences, learning objectives, deployment methods, and evaluation and measurement techniques, as well as the frequency of training.	• Is there a procedure in place to ensure that everyone in the organization receives security awareness training, including teleworkers and remote personnel? • 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? • Has the organization considered the training needs of non-employees (e.g., contractors, interns)? • Is there a need to implement information security training tailored to individual roles?

[61] See Sec. 5.2.1, *HIPAA Standard: Facility Access Controls*; Sec. 5.3.1, *HIPAA Standard: Access Control;* and Appendix F.

Key Activities	Description	Sample Questions

3. **Protection from Malicious Software, Login Monitoring, and Password Management**
 	
Implementation Specifications (All Addressable)
	• *As reasonable and appropriate, train workforce members regarding procedures for:*
	  ○ *Guarding against, detecting, and reporting malicious software;*
	  ○ *Monitoring login attempts and reporting discrepancies; and*
	  ○ *Creating, changing, and safeguarding passwords.*
	• Incorporate information concerning workforce members' roles and responsibilities in implementing these implementation specifications into training and awareness efforts.
		• Do workforce members know the importance of the timely application of system patches to protect against malicious software and the exploitation of vulnerabilities?
		• Are workforce members aware that login attempts may be monitored?
		• Do workforce members who monitor login attempts know to whom to report discrepancies?
		• Do workforce members understand their roles and responsibilities in selecting a password of appropriate strength, safeguarding their password, and changing a password when it has been compromised or is suspected of being compromised?
		• Are there policies in place that prohibit workforce members from sharing passwords with others?

4. **Develop Appropriate Awareness and Training Content, Materials, and Methods**	• Select topics to be included in the training materials, and consider current and relevant topics (e.g., phishing, email security) for the protection of ePHI. • Incorporate new information from email advisories, online IT security, daily news, websites, and periodicals, as 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, and other factors. • Training should be an ongoing, evolving process in response to environmental and operational changes that affect the security of ePHI.	• Are the topics selected for training and awareness the most relevant to the threats, vulnerabilities, and risks identified during the risk assessment? • Does the organization periodically review the topics covered in training and awareness in light of updates to the risk assessment and current threats? • Have workforce members received a copy of and do they have ready access to the organization's security procedures and policies?[62] • Do workforce members know whom to contact and how to handle a security incident?[63] • Do workforce members understand the consequences of noncompliance with the stated security policies?[64] • Do workforce members who travel, telework, or work remotely know how to handle physical laptop security issues and information security issues?[65] • Has the regulated entity researched available training resources?

[62] See Sec. 5.5.2, *HIPAA Standard: Documentation.*
[63] See Sec. 5.1.6, *HIPAA Standard: Security Incident Procedures.*
[64] See Sec. 5.1.1, *HIPAA Standard: Security Management Process.*
[65] See Sec. 5.2.4, *HIPAA Standard: Device and Media Controls.*

Key Activities	Description	Sample Questions
		• Is dedicated training staff available for the 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, video recordings, email messages, teleconferencing sessions, staff meetings, and computer-based training.	• Have all workforce members received adequate training to fulfill their security responsibilities? • Are there sanctions if workforce members do not complete the required training?
6. **Implement Security Reminders** **Implementation Specification (Addressable)**	• *Implement periodic security updates.* • Provide periodic security updates to staff, business associates, and contractors. • Consider the benefits of ongoing communication with staff (e.g., emails, newsletters) on training topics to achieve HIPAA compliance and protect ePHI.	• What methods are available or already in use to make or keep workforce members aware of security (e.g., posters, booklets, anti-phishing training)? • Is the organization making use of existing resources (e.g., from the 405(d) program or other resources listed in Appendix F) to remind staff of important security topics? • 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 the Training Plan**[66]	• Keep the security awareness and training program current. • Solicit trainee feedback to determine whether the training and awareness are successfully reaching the intended audience. • Conduct training whenever changes occur in the technology and practices, as appropriate. • Monitor the training program implementation to ensure that all workforce members participate. • Implement corrective actions when problems arise.[67]	• Are the workforce members' training and professional development programs documented and monitored, if reasonable and appropriate? • How are new workforce members trained on security? • Are new non-employees (e.g., contractors, interns) trained on security?

[66] This is also required under the HIPAA Security Rule § 164.306, General Requirements, Subsection €, *Maintenance*. See Sec. 5.1.8, *HIPAA Standard: Evaluation.*
[67] See Sec. 5.1.1, *HIPAA Standard: Security Management Process.*

5.1.6. Security Incident Procedures (§ 164.308(a)(6))[68]

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

Table 13. Key activities, descriptions, and sample questions for the Security Incident Procedures standard

Key Activities	Description	Sample Questions
1. **Determine the Goals of an 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). • Ensure that the incident response program covers all parts of the organization in which ePHI is created, stored, processed, or transmitted. • 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 lead to a breach of security? • Is there a procedure in place for reporting and handling incidents? • Has an analysis been conducted that relates reasonably anticipated organizational threats (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?[69]
2. **Develop and Deploy an Incident Response Team or Other Reasonable and Appropriate Response Mechanism**	• Determine whether 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 part of a formal incident response team if the organization has determined that implementing an incident response team is reasonable and appropriate. • Consider assigning secondary personnel to be part of the incident response team in the event that primary personnel are unavailable.	• 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?

[68] See Sec. 5.2.1, *HIPAA Standard: Facility Access Controls*; Sec. 5.3.1, *HIPAA Standard: Access Control;* and Appendix F.
[69] See Sec. 5.1.7, *HIPAA Standard: Contingency Plan.*

Key Activities	Description	Sample Questions
3. **Develop and Implement Policy and Procedures to Respond to and Report Security Incidents** **Implementation Specification (Required)**	• *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 or business associate; and document security incidents and their outcomes.* • Ensure that an organizational incident response policy[70] is in place that addresses all parts of the organization in which ePHI is created, stored, processed, or transmitted. • 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 who have roles and responsibilities related to incident response; solicit suggestions for improvements; and make changes to reflect input, if reasonable and appropriate. • Consider conducting tests of the incident response plan. • Update the procedures as required based on changing organizational needs.[71]	• Has the organization determined that maintaining a staffed security incident hotline would be reasonable and appropriate? • Has the organization developed processes for documenting and tracking incidents? • Has the organization determined reasonable and appropriate mitigation options for security incidents? • Has the organization developed standardized incident report templates to record necessary information related to incidents? • Has the organization determined that information captured in the reporting templates is reasonable and appropriate to investigate an incident? • Has the organization determined the conditions under which 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? Has a contact information list been prepared? • Has a written incident response plan been developed and provided to the incident response team? • Has the incident response plan been tested?
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. • Incidents caused by or influenced by known risks should feed back into the risk assessment process for a reevaluation of impact and/or likelihood. • Remediation and corrective action plans that arise from incidents should serve as input to the risk assessment/management process.	• Has the organization analyzed records (e.g., log files, malware) to understand the nature, extent, and scope of the incident? • Does the organization reassess risk to ePHI based on findings from this analysis? • 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 the information was gained? • Do records reflect the new contacts and resources identified for responding to an incident?

[70] See Sec. 5.5.1, *HIPAA Standard: Policies and Procedures.*
[71] See Sec. 5.5.2, *HIPAA Standard: Documentation.*

Key Activities	Description	Sample Questions
		• Does the organization consider whether current procedures were adequate for responding to a particular security incident?

5.1.7. Contingency Plan (§ 164.308(a)(7))[72]

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.*

Table 14. Key activities, descriptions, and sample questions for the Contingency Plan standard

Key Activities	Description	Sample Questions

1. **Develop a Contingency Planning Policy**[73]	• 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 critical services must be provided within specified time frames?
		  ○ 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 to determine how a failure in one system may negatively impact another one?

2. **Conduct an Applications and Data Criticality Analysis**[74] **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 that the organization can tolerate disruptions to these operations, materials, or services (e.g., due to power outages). • Evaluate the current and available levels of redundancy and geographic distribution of any storage service providers to identify risks to service availability and determine restoration times.	• 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 (e.g., cloud service providers, internet service providers, utilities, or contractors)? • What is the nature and degree of impact on the operation if any of the critical resources or service providers are not available? • Has the organization identified vendors or service providers that are critical to business operations?

[72] See Sec. 5.2.1, *HIPAA Standard: Facility Access Controls*; Sec. 5.3.1, *HIPAA Standard: Access Control;* and Appendix F.
[73] See Sec. 5.5.1, *HIPAA Standard: Policies and Procedures* and Appendix F.
[74] 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 that do not involve ePHI and other elements of an organization not covered by the HIPAA Security Rule.

Key Activities	Description	Sample Questions
	• Consider whether any vendor/service provider arrangements are critical to operations and address them as appropriate to ensure availability and reliability. • Establish cost-effective strategies for recovering these critical services or processes.	• Has the organization sufficiently addressed the availability and reliability of these services (e.g., via service-level agreements, contracts)?
3. **Identify Preventive Measures**[75]	• Identify preventive measures for each defined scenario that could result in the loss of a critical service operation involving the use of ePHI. • Ensure that 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 the loss of any critical function or resource? • What is the cost associated with the preventive measures that may be considered? • Are the preventive measures feasible (i.e., affordable and practical for the environment)? • What plans, procedures, or agreements need to be initiated to enable the implementation of the preventive measures if they are necessary?
4. **Develop Recovery Strategy**[76]	• 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 the associated priorities identified in Key Activity 2. • If part of the strategy depends on external organizations for support, ensure 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 workforce members? Have recovery procedures been documented? • Has a determination been made regarding when the plan needs to be activated (e.g., anticipated duration of outage, tolerances for outage or loss of capability, impact on service delivery)?
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? Does it address disaster recovery and data backup?[77] • Does the disaster recovery plan address what data is to be restored and in what order? • Do data backup procedures exist that include all ePHI?

[75] See Key Activities 5.1.7.5, *Data Backup Plan and Disaster Recovery Plan*, and 5.1.7.6, *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.
[76] See Key Activities 5.1.7.5, *Data Backup Plan and Disaster Recovery Plan*, and 5.1.7.6, *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.
[77] See Key Activity 5.1.7.1, Develop Contingency Planning Policy.

Key Activities	Description	Sample Questions
		• Is the frequency of backups appropriate for the environment? • Are responsibilities assigned to conduct backup activities? • Are data backup procedures documented and available to other staff? • Are backup logs reviewed and data restoration tests conducted to ensure the integrity of data backups? • Is at least one copy of the data backup stored offline to protect against corruption due to ransomware or other similar attacks? • Are backups or images of operating systems, devices, software, and configuration files necessary to support the confidentiality, integrity, and availability of ePHI included in the data backup plan?
6. **Develop and Implement an Emergency Mode Operation Plan** **Implementation Specification (Required)**	• *Establish (and implement as needed) procedures to enable the continuation of critical business processes to protect the security of ePHI while operating in emergency mode.* • "Emergency mode" operation involves only those critical business processes that must occur to protect the security of ePHI during and immediately after a crisis situation.	• Have procedures been developed to continue the critical functions identified in Key Activity 2? • 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 ePHI in that alternative mode of operation been assured?
7. **Testing and Revision Procedure** **Implementation Specification (Addressable)**	• *Implement procedures for the periodic testing and revision of contingency plans.* • Test the contingency plan on a predefined cycle (stated in the policy developed under Key Activity 1), if reasonable and appropriate. • Train those with defined plan responsibilities in their roles. • If possible, involve external entities (e.g., vendors, alternative site or service providers) in testing exercises. • Make key decisions regarding how the testing is to occur (e.g., 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 the acceptability of a sustained loss of service.	• How is the contingency plan to be tested? • Does testing lend itself to a phased approach? • Is it feasible to actually take down functions or services for the purposes of testing? • Has the organization conducted backup recovery testing to ensure that critical data can be recovered using existing data backups? • Does the backup recovery testing verify the ability to recover data and operations based on identified testing scenarios using actual tests (i.e., not tabletop exercises)? • Can testing be done during normal business hours or must it take place during off hours? • Have the tests included personnel with contingency planning responsibilities?

Key Activities	Description	Sample Questions
		• Have the results of each test been documented and any problems with the test reviewed and corrected? • If full testing is infeasible, has a tabletop scenario (e.g., a classroom-like exercise) been considered? • How frequently will the plan be tested (e.g., annually)? • When should the plan be revised?

5.1.8. Evaluation (§ 164.308(a)(8))[78]

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 a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.*

Table 15. Key activities, descriptions, and sample questions for the Evaluation standard

Key Activities	Description	Sample Questions
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 are 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? • Are the evaluators sufficiently independent to provide objective reporting? • How much training will staff need on security-related technical and non-technical 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**[79]	• Develop and document organizational policies and procedures[80] for conducting evaluation. • Once security controls have been implemented in response to the organization's risk assessment and management processes, periodically review these implemented security measures to ensure their continued effectiveness in protecting ePHI. • Consider determining any specific evaluation metrics and/or measurements to be captured during evaluation.	• Has the organization documented policies and procedures for conducting the evaluation of security controls? • Have management, operational, and technical issues been considered? • Do the elements of each evaluation procedure (e.g., questions, statements, or other components) address individual, measurable security safeguards for ePHI? • Has the organization developed evaluation procedures that capture any desired metrics or measurements?

[78] See Sec. 5.2.1, *HIPAA Standard: Facility Access Controls*, and Sec. 5.3.1, *HIPAA Standard: Access Control.*
[79] Organizations may wish to review and employ, where reasonable and appropriate, security control assessment procedures found in NIST [SP 800-53A], Rev.5, *Assessing Security and Privacy Controls in Information Systems and Organizations*.
[80] See Sec. 5.5.1, *HIPAA Standard: Policies and Procedures.*

Key Activities	Description	Sample Questions
	Metrics and/or measurements can assist in tracking progress over time. • 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 the compliance, integration, or maturity of a particular security safeguard deployed to protect 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? • Does the evaluation tool address the protection of ePHI that is collected, used, or disclosed?
3. **Conduct Evaluation**	• Determine in advance what departments and/or staff will participate in the evaluation. • Determine what constitutes an environmental or operational change that affects the security of ePHI. • Determine when evaluations are conducted in response to an environmental or operational change that affects the security of ePHI (e.g., prior to the change, contemporaneous with the change, after the change). • Secure management support for the evaluation process to ensure participation. • Collect and document all needed information. Collection methods may include the use of interviews, surveys, and the outputs of automated tools, such as access control auditing tools, system logs, and the results of penetration testing. • Conduct penetration testing (where testers attempt to compromise system security for the sole purpose of testing the effectiveness of security controls), if reasonable and appropriate. • Evaluation may include reviewing organizational policies and procedures, assessing the implementation of security	• If available, have staff members with knowledge of IT security been consulted and included in the evaluation team? • Are appropriate personnel notified of planned environmental or operational changes that could affect the security of ePHI? • Is a change management process in place that includes identification and communication of environmental and operational changes that could affect the security of ePHI? • If penetration testing has been 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 explored the use of automated tools to support the evaluation process?

Key Activities	Description	Sample Questions
	controls, collecting evidence of security control implementation, and performing physical walk-throughs.	
4. **Document Results**[81]	• Document each evaluation finding as well as remediation options, recommendations, and decisions. • Document known gaps between identified risks, mitigating security controls, and any acceptance of risk, including justification. • Develop security program priorities and establish targets for continuous improvement. • Utilize the results of evaluations to inform impactful security changes to protect ePHI. • Communicate evaluation results, metrics, and/or measurements to relevant organizational personnel.	• Does the process support the development of security recommendations? • When 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? • Does the organization use evaluation results to enhance the protection of ePHI rather than for the sake of compliance?
5. **Repeat Evaluations Periodically**	• Establish the frequency of evaluations. Consider the sensitivity of the ePHI controlled by the organization as well as the organization's size, complexity, and environmental and/or operational changes (e.g., other relevant laws or accreditation requirements). • In addition to periodic reevaluations, consider repeating evaluations when environmental and operational changes that affect the security of ePHI are made to the organization (e.g., if new technology is adopted or if there are newly recognized risks to the security of ePHI).	• 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 the frequency of security evaluations reflect any and all relevant federal or state laws that bear on environmental or operational changes affecting the security of ePHI? • Has the organization explored the use of automated tools to support periodic evaluations?

[81] See Sec. 5.5.2, *HIPAA Standard: Documentation*.

5.1.9. Business Associate Contracts and Other Arrangements (§ 164.308(b)(1))[82]

HIPAA Standard: *A covered entity 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. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.*

Covered entities need to be cognizant of differentiating between best practices versus what the Security Rule requires. Vendor management and supply chain risks are important topics due to the potential they have to introduce new threats and risks to organizations. However, to the extent that such vendors and service providers are business associates, HIPAA treats them the same as covered entities with respect to Security Rule compliance. Covered entities and business associates are required to obtain written satisfactory assurances that PHI will be protected. Covered entities and business associates are permitted to require more of their business associates and even include more stringent cybersecurity requirements in a business associate agreement (BAA). These requirements would need to be agreed upon by both the covered entity and the business associate.

Table 16. Key activities, descriptions, and sample questions for the Business Associate Contracts and Other Arrangements standard

Key Activities	Description	Sample Questions
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. • Business associates must have a BAA in place with each of their subcontractor business associates. Subcontractor business associates are also directly liable for their own Security Rule violations.	• Does each written and executed BAA contain sufficient language to ensure that ePHI and any other required information types will be protected? • Have all organizations or vendors that provide a service or function on behalf of the organization been identified? Such services may include: ○ Cloud service providers ○ Claims processing or billing ○ Data analysis ○ Utilization review ○ Quality assurance ○ Benefit management ○ Practice management ○ Re-pricing ○ Hardware/software maintenance ○ All other HIPAA-regulated functions

[82] See Sec. 5.4.1, *HIPAA Standard: Business Associate Contracts or Other Arrangements*.

Key Activities	Description	Sample Questions
		• Have outsourced functions that involve the use of ePHI been considered? Such functions may include: ○ Actuarial services ○ Data storage and/or aggregation ○ Administrative services ○ Accreditation ○ Financial services ○ IT support
2. **Establish a Process for Measuring Contract Performance and Terminating the Contract if Security Requirements Are Not Being Met**[83]	• Maintain clear lines of communication between covered entities and business associates regarding the protection of ePHI per the BAA or contract. • Establish criteria for measuring contract performance.	• What is the service being performed? • What is the expected outcome? • Is there a process for reporting security incidents related to the agreement? • Are additional assurances of protections for ePHI from the business associate necessary? If so, where will such additional assurances be documented (e.g., in the BAA, service-level agreement, or other documentation)? and how will they be met (e.g., providing documentation of implemented safeguards, audits, certifications)?
3. **Written Contract or Other Arrangement** **Implementation Specification (Required)**	• *Document the satisfactory assurances required by this standard through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).*[84] Readers may find useful resources in Appendix F, including OCR BAA guidance and/or templates that include applicable language. • Execute new or update existing agreements or arrangements, as appropriate. • Identify roles and responsibilities. • Include security requirements in business associate contracts and agreements to address the confidentiality, integrity, and availability of ePHI. • Specify any training requirements associated with the contract/agreement or arrangement, if reasonable and appropriate.	• Who is responsible for coordinating and preparing the final agreement or arrangement? • Does the agreement or arrangement specify how information is to be transmitted to and from the business associate? • Have security controls been specified for the business associate? • Are clear responsibilities identified and established regarding potentially overlapping HIPAA obligations (e.g., if hosting ePHI in the cloud, will the covered entity, business associate, or both address encryption)? • Have appropriate organizational personnel been trained in the process of initiating and maintaining a business associate agreement (BAA)?

[83] See Sec. 5.4.1, *HIPAA Standard: Business Associate Contracts or Other Arrangements.*
[84] See Sec. 5.4.1, *HIPAA Standard: Business Associate Contracts or Other Arrangements*.

5.2. Physical Safeguards

5.2.1. Facility Access Controls (§ 164.310(a))[85]

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.*

Table 17. Key activities, descriptions, and sample questions for the Facility Access Controls standard

Key Activities	Description	Sample Questions

1. **Conduct an Analysis of Existing Physical Security Vulnerabilities**[86] [87]	• Inventory facilities and identify shortfalls and/or vulnerabilities in current physical security capabilities.
	• Assign degrees of significance to each vulnerability identified and ensure that proper access is allowed.
	• Determine which types of facilities require access controls to safeguard ePHI, such as:
	  ○ Data centers
	  ○ Peripheral equipment locations (e.g., wiring closets, storage areas, exam rooms)
	  ○ IT staff offices
	  ○ Workstation locations
		• If reasonable and appropriate, do non-public areas have locks and cameras?
		• Are computing devices protected from public access or viewing?[88]
		• 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 human-made disasters that could happen in the environment?[89]
		• Do normal physical protections exist (e.g., locks on doors, windows, and other means of preventing unauthorized access)?
		• Are network wiring cables protected and not exposed to unauthorized personnel?
		• Is there a list of workforce members who can access the facility after hours via the use of keys, badge access, and knowledge of the security or alarm system?

[85] See Sec. 5.3.1, *HIPAA Standard: Access Control.*
[86] This key activity may be performed as part of the risk analysis implementation specification. See Sec. 5.1.1, *HIPAA Standard: Security Management Process.*
[87] See Key Activity 5.2.1.3, *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.
[88] See Sec. 5.2.2, *HIPAA Standard: Workstation Use.*
[89] See Sec. 5.1.7, *HIPAA Standard: Contingency Plan.*

Key Activities	Description	Sample Questions
2. **Identify Corrective Measures**[90] [91]	• Identify and assign responsibility for the measures and activities necessary to correct deficiencies and ensure that proper physical 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 that proper access is allowed.	• Who is responsible for security?[92] • 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?[93] • How will decisions and actions be documented?[94] • Is a property owner or external party (e.g., cloud service provider) required to make physical changes to meet the requirements?
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 regulated entity's possession.[95] • Include documentation of the facility inventory, physical maintenance records, and a 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 (e.g., exterior, interior, equipment, access controls, maintenance records)? • 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?[96]
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.*	• What are the policies and procedures in place for controlling access by staff, contractors, visitors, and probationary employees? • Do the procedures identify individuals, roles, or job functions that are authorized to access software programs for testing and revision?

[90] This key activity may be performed as part of the risk management implementation specification. See Sec. 5.1.1, *HIPAA Standard: Security Management Process.*
[91] See Key Activity 5.2.1.3, *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.
[92] See Sec. 5.1.2, *HIPAA Standard: Assigned Security Responsibility.*
[93] See Sec. 5.1.5, *HIPAA Standard: Security Awareness and Training.*
[94] See Sec. 5.5.2, *HIPAA Standard: Documentation.*
[95] Note that a business associate is responsible for implementing appropriate physical security measures for its own facilities. Business associates should approach these key activities, descriptions, and sample questions from the perspective of their own facilities. A covered entity requires written satisfactory assurances that ePHI will be protected by the business associate.
[96] See Sec. 5.1.7, *HIPAA Standard: Contingency Plan.*

Key Activities	Description	Sample Questions
	• Implement procedures to provide facility access to authorized personnel and visitors and exclude unauthorized persons.	• How many access points exist in each facility? Is there an inventory? • Is monitoring equipment necessary? • Is there a periodic review of personnel with physical access?
5. **Establish Contingency Operations Procedures** **Implementation Specification (Addressable)**	• *Establish (and implement as needed) procedures that allow facility access in support of the restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operations Plan in the event of an emergency.*	• Are there procedures to allow facility access while restoring lost data 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 or unit? • Will the contingency plan be appropriate in the event of all types of potential disasters (e.g., fire, flood, earthquake)?
6. **Maintain Maintenance Records**[97] **Implementation Specification (Addressable)**	• *Implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (e.g., hardware, walls, doors, and locks).*	• Are policies and procedures developed and implemented that specify how to document repairs and modifications to the physical components of a facility that are related to security? • Are records of repairs to hardware, walls, doors, and locks maintained? • Has responsibility for maintaining these records been assigned?

[97] See Sec. 5.5.2, *HIPAA Standard: Documentation.*

5.2.2. 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*.

Table 18. Key activities, descriptions, and sample questions for the Workstation Use standard

Key Activities	Description	Sample Questions
1. **Identify Workstation and Device Types and Functions or Uses**	• Inventory workstations and devices that create, store, process, or transmit ePHI. Be sure to consider the multitude of computing devices (e.g., medical equipment, IoT devices, tablets, smart phones). • Develop policies and procedures for each type of device and identify and accommodate their unique issues. • Classify devices based on the capabilities, connections, and allowable activities for each device used. • Determine the proper function and manner by which specific workstations or classes of workstations are permitted to access ePHI (e.g., applications permitting access to ePHI that are allowed on workstations used by a hospital's customer service call center or its radiology department).	• Do the policies and procedures identify devices that access ePHI and those that do not? • Is there an inventory of device types and locations in the organization? • Who is responsible for this inventory and its maintenance? • What tasks are commonly performed on a given device or type of device? • Are all types of computing devices used as workstations identified along with the use of these devices? • Are all devices that create, store, process, or transmit ePHI owned by the regulated entity? • Are some devices personally owned or owned by another party? • Has the organization considered the use of automation to manage device inventory?
2. **Identify the Expected Performance of Each Type of Workstation and Device**	• Develop and document policies and procedures related to the proper use and performance of devices that create, store, process, or transmit ePHI.	• How are these devices used in day-to-day operations? • Which devices are involved in various work activities? • What are key operational risks that could result in a breach of security? • Do the policies and procedures address the use of these devices for any personal use? • Has the organization updated training and awareness content to include the proper use and performance of these devices?

3. **Analyze Physical Surroundings for Physical Attributes**[98]	• Ensure that any risks associated with a device's surroundings are known and analyzed for possible negative impacts. • Develop policies and procedures that will prevent or preclude the unauthorized access of unattended devices, limit the ability of unauthorized persons to view sensitive information, and dispose of sensitive information as needed.	• Do the policies and procedures specify where to place devices to only allow viewing by authorized personnel? • Where are devices located? • Where does work on ePHI occur? • Are some devices stationary? • Are some devices mobile and leave the physical facility? • Is viewing by unauthorized individuals restricted or limited on these devices? • Do changes need to be made in the space configuration? • Do workforce members understand the security requirements for the data they use in their day-to-day jobs? • Are any computing components (e.g., servers, workstations. medical devices) kept in locations that put the confidentiality, integrity, and availability of ePHI at risk?

[98] See Sec. 5.1.5, *HIPAA Standard: Security Awareness and Training.* This key activity should be performed during security training or awareness activities.

5.2.3. 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.*

Table 19. Key activities, descriptions, and sample questions for the Workstation Security standard

Key Activities	Description	Sample Questions
1. **Identify All Methods of Physical Access to Workstations and Devices**	• Document the different ways that users access workstations and other devices that create, store, process, or transmit ePHI. Be sure to consider the multitude of computing devices (e.g., medical equipment, IoT devices, tablets, smart phones). • Consider any mobile devices that leave the physical facility as well as remote workers who access devices that create, store, process, or transmit ePHI.	• Is there an inventory of all current device locations? • Are any devices located in public areas? • Are laptops or other computing devices used as workstations to create, access, store, process, or transmit ePHI?
2. **Analyze the Risks Associated with Each Type of Access**[99]	• Determine which type of access identified in Key Activity 1 poses the greatest threat to the security of ePHI.	• Do any devices leave the facility? • Are any devices housed in areas that are more vulnerable to unauthorized use, theft, or viewing of the data they contain? • What are the options for modifying the current access configuration to protect ePHI?

3. **Identify and Implement Physical Safeguards for Workstations and Devices**	• Implement physical safeguards and other security measures to minimize the possibility of inappropriate access to ePHI through computing devices.
	• If there are impediments to physically securing devices and/or the facilities where devices are located, additional safeguards should be considered, such as:
	  ○ Limiting device capabilities to access ePHI
	  ○ Limiting user permissions to access ePHI
	  ○ Device encryption
	  ○ Stringent access controls (e.g., multi-factor authentication [MFA])
	  ○ Screen lock
		• Are physical safeguards implemented for all devices that access ePHI to restrict access to authorized users?
		• Are devices and other tools used in the provisioning of treatment, payment, and operations protected from unauthorized access, viewing, modification, and/or theft within mobile healthcare environments?
		• What safeguards are in place,(e.g., locked doors, screen barriers, cameras, guards)?[100]
		• Are additional physical safeguards needed to protect devices with ePHI?
		• Do any devices need to be relocated to enhance physical security?

[99] This key activity may be conducted pursuant to the risk analysis and risk management implementation specifications of the security management process standard. See Sec. 5.1.1, *HIPAA Standard: Security Management Process.*

[100] See Sec. 5.1.1, *HIPAA Standard: Security Management Process.*

	○ Device management (e.g., mobile device management [MDM], endpoint detection and response [EDR]) ○ Workforce education and training related to mobile and remote computing risks to ePHI	• Are safeguards such as anti-theft devices, physical privacy screens, or other procedures used to help prevent unauthorized audio and video recording? • Have workforce members been trained on security?[101] • Are some devices not owned by the organization? Do these ownership considerations preclude the use of any physical security controls on the device? • Do the policies and procedures specify the use of additional security measures to protect devices with ePHI, such as using privacy screens, enabling password-protected screen savers, or logging off the device?

[101] See Sec. 5.1.5, *HIPAA Standard: Security Awareness and Training.*

5.2.4. Device and Media Controls (§ 164.310(d))

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.*

Table 20. Key activities, descriptions, and sample questions for the Device and Media Controls standard

Key Activities	Description	Sample Questions
1. **Implement Methods for the 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. • Ensure that ePHI is properly destroyed and cannot be recreated.	• What ePHI is created, stored, processed, and transmitted by the organization? On what media is it located? • Is data stored on removable, reusable media (e.g., flash drives, Secure Digital [SD] memory cards)? • Are policies and procedures developed and implemented that address the disposal of ePHI and/or the hardware and media on which ePHI is stored? • Is there a process for destroying data on all media? • What are the options for disposing of data on hardware? What are the costs? • Prior to disposal, have media and devices containing ePHI been sanitized in accordance with [SP 800-88]?
2. **Develop and Implement Procedures for the Reuse of Electronic Media** **Implementation Specification (Required)**	• *Implement procedures for the removal of ePHI from electronic media before the media become available for reuse.* • Ensure that ePHI previously stored on any electronic media cannot be accessed and reused. • Identify removable media and their uses. • Ensure that ePHI is removed from reusable media before they are used to record new information.	• Do policies and procedures already exist regarding the reuse of electronic media (i.e., hardware and software)? • Have reused media been erased to the point where previous ePHI is neither readily available nor recoverable? • Is one individual and/or department responsible for coordinating the disposal of data and the reuse of the hardware and software? • Are workforce members appropriately trained on the security risks to ePHI when reusing software and hardware?[102]
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 for them.* • Ensure that ePHI is not inadvertently released or shared with any unauthorized party.	• Have policies and procedures been implemented that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility and the movement of these items within the facility?

[102] See Sec. 5.1.5, *HIPAA Standard: Security Awareness and Training.*

Key Activities	Description	Sample Questions
	• Ensure that an individual is responsible for and records the receipt and removal of hardware and software with ePHI.	• Has a process been implemented to maintain a record of the movements of and persons responsible for hardware and electronic media that contain ePHI? • Where is data stored (i.e., what type of media)? • What procedures already exist to track hardware and software within the organization (e.g., an enterprise inventory management system)? • 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 (Addressable)**	• *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 maintain the integrity of ePHI during equipment relocation.	• Has a process been implemented to create a retrievable, exact copy of ePHI when needed and before the movement of equipment? • Are backup files maintained off-site to ensure data availability in the event that data is lost while transporting or moving electronic media that contain ePHI? • If data were to be unavailable while media are transported or moved for a period of time, what would the business impact be?

5.3. Technical Safeguards

5.3.1. Access Control (§ 164.312(a))

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).*

Table 21. Key activities, descriptions, and sample questions for the Access Control standard

Key Activities	Description	Sample Questions
1. **Analyze Workloads and Operations to Identify the Access Needs of All Users**[103]	• Identify an approach[104] for access control. • Consider all applications and systems containing ePHI that should only be available to authorized users, processes, and services. • Integrate these activities into the access granting and management process.[105]	• Have all applications and systems with ePHI been identified? • What user roles are defined for those applications and systems? • Is access to systems that contain ePHI only granted to authorized processes and services? • Where is the ePHI supporting those applications and systems currently housed (e.g., stand-alone computer, network storage, database)? • Are data and/or systems being accessed remotely? • Have access decisions been based on determinations from § 164.308(a)(4) Information Access Management?
2. **Identify Technical Access Control Capabilities**	• Determine the access control capabilities of all systems with ePHI. • Determine whether network infrastructure can limit access to systems with ePHI (e.g., network segmentation). • Implement technical access controls to limit access to ePHI to only that which has been granted in accordance with the regulated entity's information access management policies and procedures (see 45 CFR 164.308(a)(4)).	• How are the systems accessed for viewing, modifying, or creating data? • Can identified technical access controls limit access to ePHI to only what is authorized in accordance with the regulated entity's information access management policies and procedures (see 45 CFR 164.308(a)(4))?

[103] See Sec. 5.1.4, *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 processes detailed in the Information Access Management standard.
[104] Consider how zero trust architecture principals can aid in the organization's approach to access control. See Appendix F for more information.
[105] See Sec. 5.1.4, *HIPAA Standard: Information Access Management.*

Key Activities	Description	Sample Questions
3. **Ensure That All System Users Have Been Assigned a Unique Identifier**[106] **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.[107]	• How should the identifier be established (e.g., length and content)? • Should the identifier be self-selected, organizationally selected, or randomly generated? • Are logs associated with access events created? • Are these access logs regularly reviewed? • Can the unique user identifier be used to track user access to ePHI?
4. **Develop Access Control Policy**[108] **and Procedures**	• Establish a formal policy for access control that will guide the development of procedures.[109] • Specify requirements for access control that are both feasible and cost-effective.[110]	• Have rules of behavior been established and communicated to system users? • How will rules of behavior be enforced?
5. **Implement Access Control Procedures Using Selected Hardware and Software**	• Implement the policy and procedures using existing or additional hardware or software solutions.	• Who will manage the access control procedures? • Are current users trained in access control management?[111] • Will user training be needed to implement access control procedures? • Do the medical devices in use by the organization support user authentication? Are there processes in place to manage this authentication?

[106] See Appendix F for information and resources related to Identity Management.
[107] See Sec. 5.3.2, *HIPAA Standard: Audit Controls.*
[108] See Sec. 5.1.4, *HIPAA Standard: Information Access Management.*
[109] See Sec. 5.1.4, *HIPAA Standard: Information Access Management.*
[110] See Sec. 5.1.1, *HIPAA Standard: Security Management Process.*
[111] See Sec. 5.1.5, *HIPAA Standard: Security Awareness and Training.*

Key Activities	Description	Sample Questions

6. **Review and Update Access for Users and Processes**	• Enforce the policy and procedures as a matter of ongoing operations.[112]
	• Determine whether any changes are needed for access control mechanisms.
	• Ensure that the modification of technical controls that affect a user's access to ePHI continue to limit access to ePHI to that which has been granted in accordance with the regulated entity's information access management policies and procedures (see 45 CFR 164.308(a)(4)).
	• Establish procedures for updating access when users require the following:[113]
	  ○ Initial access
	  ○ Increased access
	  ○ Access to different systems or applications than those they currently have
		• Have new workforce members/users been given proper instructions for protecting data and systems?[114]
		• What are the procedures for new workforce member/user access to data and systems?[115]
		• Are there procedures for reviewing and, if appropriate, modifying access authorizations for existing users, services, and processes?[116]
		• Do users and processes have the appropriate set of permissions to ePHI to which they were granted access and to the appropriate systems that create, store, process, or transmit ePHI?
		• Has the regulated entity considered the use of automation for reviewing the access needs of users and processes?

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 for supporting continuity of operations should the normal access procedures be disabled or unavailable due to system problems.	• Are there policies and procedures in place to provide appropriate access to ePHI in emergency situations? • When should the emergency access procedure be activated? • Who is authorized to make the decision?[117] • Who has assigned roles in the process?[118] • 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**	• Consider whether the addressable implementation specifications of this standard are reasonable and appropriate:	• Are automatic logoff features available for any of the regulated entity's operating systems or other major applications?

[112] See Sec. 5.1.4, *HIPAA Standard: Information Access Management.*
[113] See Sec. 5.1.4, *HIPAA Standard: Information Access Management.*
[114] See Sec. 5.1.5, *HIPAA Standard: Security Awareness and Training.*
[115] See Sec. 5.1.4, *HIPAA Standard: Information Access Management.*
[116] See Sec. 5.1.4, *HIPAA Standard: Information Access Management.*
[117] See Sec. 5.1.7, *HIPAA Standard: Contingency Plan.*
[118] See Sec. 5.1.7, *HIPAA Standard: Contingency Plan.*

Key Activities	Description	Sample Questions
Implementation Specifications (Both Addressable)	○ *Implement electronic procedures that terminate an electronic session after a predetermined period of inactivity.* ○ *Implement a mechanism to encrypt and decrypt ePHI.*	• If applications have been created or developed in-house, is it reasonable and appropriate to modify them to feature an automatic logoff capability? • What period of inactivity prior to automatic logoff is reasonable and appropriate for the regulated entity? • What encryption capabilities are available for the regulated entity's ePHI? • Is encryption appropriate for storing and maintaining ePHI (i.e., at rest)? • Based on the risk assessment, is encryption needed to effectively protect ePHI at rest from unauthorized access? • Is email encryption necessary for the organization to protect ePHI? • Are automated confidentiality statements needed for email leaving the organization?
9. **Terminate Access if it is No Longer Required**[119]	• Ensure that access to ePHI is terminated if the access is no longer authorized. • Consider implementing a user recertification process to ensure that least privilege is enforced.	• Are rules being enforced to remove access by workforce members who no longer have a need to know because they have changed assignments or have stopped working for the organization? • Does the organization revisit user access requirements regularly to ensure least privilege?

[119] See Sec. 5.1.3, *HIPAA Standard: Workforce Security.*

5.3.2. 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.*

Table 22. Key activities, descriptions, and sample questions for the Audit Controls standard

Key Activities	Description	Sample Questions
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 regulated entity's risk assessment and other organizational factors.[120] • Determine what activities need to be captured using the results of the risk assessment and risk management processes.	• Where is ePHI at risk in the organization?[121] • What systems, applications, or processes make ePHI vulnerable to unauthorized or inappropriate tampering, uses, or disclosures?[122] • What activities will be audited (e.g., creating ePHI, accessing ePHI, modifying ePHI, transmitting ePHI, and/or deleting files or records that contain ePHI)? • What should the audit record include (e.g., user responsible for the activity; event type, date, or time)? • Are audit records generated for all systems/devices that create, store, process, or transmit ePHI?
2. **Select the Tools That Will Be Deployed for Auditing and System Activity Reviews**	• Evaluate existing system capabilities and determine whether any changes or upgrades are necessary.	• What tools are in place? • What are the most appropriate monitoring tools for the organization (e.g., 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 organization's decisions on audits and reviews.	• 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?[123] • Where will audit information reside (e.g., separate server)?

[120] See Sec. 5.1.1, *HIPAA Standard: Security Management Process*, and Key Activity 5.1.1.7, *Develop and Deploy the Information System Activity Review Process.*
[121] See Sec. 5.1.1, *HIPAA Standard: Security Management Process*, and Key Activity 5.1.1.2, *Conduct Risk Assessment.*
[122] See Sec. 5.1.1, *HIPAA Standard: Security Management Process*, and Key Activity 5.1.1.2, *Conduct Risk Assessment.*
[123] See Sec. 5.1.1, *HIPAA Standard: Security Management Process*, and Key Activity 5.1.1.6, *Develop and Implement a Sanction Policy*.

Key Activities	Description	Sample Questions
4. **Develop Appropriate Standard Operating Procedures**[124]	• Determine the types of audit trail data and monitoring procedures that will be needed to derive exception reports. • Determine the frequency of audit log reviews based on the risk assessment and risk management processes.	• How will exception reports or logs be reviewed? • Has the organization considered the use of automation to assist in the monitoring and review of system activity? • Are the organization's monitoring system activity and logs reviewed frequently enough to sufficiently protect ePHI? • Where will monitoring reports be filed and maintained? • Is there a formal process in place to address system misuse, abuse, and fraudulent activity?[125] • How will managers and employees be notified, when appropriate, regarding suspect activity?
5. **Implement the Audit/System Activity Review Process**[126]	• Activate the necessary audit system. • Begin logging and auditing procedures.	• What mechanisms (e.g., metrics) will be implemented to assess the effectiveness of the audit process? • What is the plan to revise the audit process when needed?

[124] See Sec. 5.1.1, *HIPAA Standard: Security Management Process*, and Key Activity 5.1.1.7, *Develop and Deploy the Information system Activity Review Process*.
[125] See Sec. 5.1.1, *HIPAA Standard: Security Management Process*, and Key Activity 5.1.1.6, *Develop and Implement a Sanction Policy*.
[126] See Sec. 5.1.1, *HIPAA Standard: Security Management Process*, and Key Activity 5.1.1.9, *Implement the Information System Activity Review and Audit Process.*

5.3.3. Integrity (§ 164.312(c))

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

Table 23. Key activities, descriptions, and sample questions for the Integrity standard

Key Activities	Description	Sample Questions
1. **Identify All Users Who Have Been Authorized to Access ePHI**[127]	• Identify all approved users with the ability to alter or destroy ePHI, if reasonable and appropriate. • Address this Key Activity in conjunction with the identification of unauthorized sources in Key Activity 2.	• How are users authorized to access the information?[128] • Is there a sound basis for why they need the access?[129] • Have they been trained on how to use the information?[130] • Is there an audit trail established for all accesses to the information?[131]
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, ransomware, insider threats, business competitors, user errors).[132] • Conduct this activity as part of a risk analysis.[133] • Consider how the organization will detect unauthorized modification to ePHI.	• What are likely sources that could jeopardize information integrity?[134] • 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 prevent alteration of the information during transmission?[135] • What options exist to detect the unauthorized modification of ePHI?
3. **Develop the Integrity Policy and Requirements**	• Establish a formal written set of integrity requirements based on the results of the analysis completed in Key Activities 1 and 2.	• 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 personnel?

[127] See Sec. 5.1.3, *HIPAA Standard: Workforce Security*; Sec. 5.3.1, *HIPAA Standard: Access Control*; and Sec. 5.5.1, *HIPAA Standard: Policies and Procedures.*
[128] See Sec. 5.1.3, *HIPAA Standard: Workforce Security*, and Sec. 5.3.1, *HIPAA Standard: Access Control.*
[129] See Sec. 5.1.3, *HIPAA Standard: Workforce Security.*
[130] See Sec. 5.1.5, *HIPAA Standard: Security Awareness and Training.*
[131] See Sec. 5.3.2, *HIPAA Standard: Audit Controls.*
[132] See Sec. 5.1.1, *HIPAA Standard: Security Management Process.*
[133] See Sec. 5.1.1, *HIPAA Standard: Security Management Process.*
[134] See Sec. 5.1.1, *HIPAA Standard: Security Management Process.*
[135] See Sec. 5.1.1, *HIPAA Standard: Security Management Process*, and Sec. 5.3.5, *HIPAA Standard: Transmission Security.*

Key Activities	Description	Sample Questions
4. **Implement Procedures to Address These Requirements**	• Identify and implement methods that will be used to protect ePHI from unauthorized modification. • Identify and implement tools and techniques to be developed or procured that support the assurance of integrity.	• Are current audit, logging, and access control techniques sufficient to address the integrity of ePHI? • If not, what additional techniques (e.g., quality control process, transaction and output reconstruction) can be utilized to check the integrity of ePHI? • Are technical solutions in place to prevent and detect the malicious alteration or destruction of ePHI (e.g., anti-malware, anti-ransomware, file integrity monitoring solutions)? • Can the 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 mechanisms for integrity verification, such as:
	  ○ Error-correcting memory
	  ○ Digital signatures
		• Are the uses 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?
		• If ePHI is detected as altered by unauthorized users or improperly altered by authorized users, is a process in place to respond?
		• Is this response process tied to organizational incident management processes?

6. **Establish a Monitoring Process to Assess How the Implemented Process is Working**	• Review existing processes to determine whether objectives are being addressed.[136] • Continually reassess integrity processes as technology and operational environments change to determine whether they need to be revised.[137]	• Are there reported instances of information integrity problems? Have they decreased since integrity procedures were implemented?[138] • Does the process, as implemented, provide a higher level of assurance that information integrity is being maintained?

[136] See Sec. 5.1.8, *HIPAA Standard: Evaluation.*
[137] See Sec. 5.1.8, *HIPAA Standard: Evaluation.*
[138] See Sec. 5.1.6, *HIPAA Standard: Security Incident Procedures.*

5.3.4. Person or Entity Authentication (§ 164.312(d))[139]

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

Table 24. Key activities, descriptions, and sample questions for the Person or Entity Authentication standard

Key Activities	Description	Sample Questions
1. **Determine Authentication Applicability to Current Systems/Applications**	• Identify the methods available for authentication. Under the HIPAA Security Rule, authentication is the corroboration that a person is the one claimed (45 CFR § 164.304). • Identify points of electronic access that require or should require authentication. Ensure that the regulated entity's risk analysis properly assesses risks for such access points (e.g., risks of unauthorized access from within the enterprise could be different than those of remote unauthorized access). • Authentication requires establishing the validity of a transmission source and/or verifying an individual's claim that they have 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? • Can risks of unauthorized access be sufficiently reduced for each point of electronic access with available authentication methods? • What will it cost to implement the available methods in the environment? • Are there trained staff who can maintain the system or should outsourced support be considered? • Are passwords being used? If so, are they unique to the individual? • Is MFA being used? If so, how and where is it implemented?
2. **Evaluate Available Authentication Options**	• Weigh the relative advantages and disadvantages of commonly used authentication approaches. • There are three commonly used authentication approaches available: 1. Something a person knows, such as a password 2. Something a person has or is in possession of, such as a token (e.g., smart card, hardware token) 3. Some type of biometric identification that a person provides, such as a fingerprint • MFA utilizes two or more authentication approaches to enforce stronger authentication. • Consider implementing MFA solutions[140] when the risk to ePHI is sufficiently high.	• What are the strengths and weaknesses of each available option? • Which can be best supported with assigned resources (e.g., budget/staffing)? • What level of authentication is appropriate for each access to ePHI based on the assessment of risk? • Has the organization identified all instances of access to ePHI (including by services, vendors, or application programming interfaces [APIs]) and considered appropriate authentication requirements based on the risk assessment?

[139] See Sec. 5.3.1, *HIPAA Standard: Access Control*; Sec. 5.3.2, *HIPAA Standard: Audit Controls*; and [SP 800-63B], *Digital Identity Guidelines: Authentication and Lifecycle Management*.
[140] Some MFA implementations may offer greater protection than others. Consider the pros and cons of each MFA option in light of the risk to ePHI.

Key Activities	Description	Sample Questions
		• Has the organization considered MFA for access to ePHI that poses high risk (e.g., remote access, access to privileged functions)? • Has the organization researched available MFA options and made a selection based on risk to ePHI? • Is outside vendor support required to implement the process? • Are there password-less authentication options (e.g., biometric authentication) available that can sufficiently address the risk to ePHI?
3. **Select and Implement Authentication Options**	• Consider the results of the analysis conducted under Key Activity 2 and select appropriate authentication methods based on the results of the risk assessment and risk management processes. • Implement the methods selected in organizational operations and activities.	• Has the organization's selection of authentication methods been made based on the results of the risk assessment? • If passwords are being used as an authentication element, are they of sufficient length and strength to protect ePHI? Is this enforced by technical policies? • Has necessary user and support staff training[141] been completed? • Have a 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 compromise the authentication information (e.g., password file encryption)?

[141] See Section 5.1.5, *HIPAA Standard: Security Awareness and Training.*

5.3.5. 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*.

Table 25. Key activities, descriptions, and sample questions for the Transmission Security standard

Key Activities	Description	Sample Questions
1. **Identify Any Possible Unauthorized Sources That May Be Able to Intercept and/or Modify the Information**	• Identify all pathways by which ePHI will be transmitted into, within, and outside of the organization. • Identify scenarios (e.g., telehealth, claims processing) that may result in access to or modification of the ePHI by unauthorized sources during transmission (e.g., hackers, disgruntled employees, business competitors).[142] • Identify scenarios and pathways that may put ePHI at a high level of risk.	• Have all pathways by which ePHI will be transmitted (e.g., file transfers, email, web portals, mobile apps, communications with servers or databases containing ePHI, online tracking) been identified? • Has a risk assessment been used to determine transmission pathways and scenarios that may pose high risk to ePHI? • What measures exist to protect ePHI in transmission? • Have appropriate protection mechanisms been identified for all scenarios and pathways by which ePHI is transmitted? • Is there an auditing process in place to verify that ePHI has been protected against unauthorized access during transmission?[143] • Are there trained workforce 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?

[142] See Sec. 5.1.7, *HIPAA Standard: Contingency Plan*, and Sec. 5.1.1, *HIPAA Standard: Security Management Process.*
[143] See Sec. 5.1.1, *HIPAA Standard: Security Management Process.*

Key Activities	Description	Sample Questions
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 security measures are currently used to protect ePHI during transmission? • 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 appropriate.*	• Is encryption reasonable and appropriate to protect ePHI in transmission? • Based on the risk assessment, is encryption needed to effectively protect the information from unauthorized access during transmission? • Has the organization considered the use of email encryption and automated confidentiality statements when emailing outside of the organization? • Is encryption feasible and cost-effective in this environment? • What encryption algorithms and mechanisms are available? • Are available encryption algorithms and mechanisms of sufficient strength to protect electronically transmitted ePHI? • Is electronic transmission hardware/software configured so that the strength of encryption used in transmitting ePHI cannot be weakened? • Have all applications used on devices that support the provisioning of health services been assessed to verify that strong transmission security is implemented? • Does the covered entity have the appropriate staff to maintain a process for encrypting ePHI during transmission? • Are workforce members skilled in the use of encryption?

5.4. Organizational Requirements

5.4.1. Business Associate Contracts or Other Arrangements (§ 164.314(a))

HIPAA Standard: *(i) The contract or other arrangement between the covered entity and its business associate required by § 164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable. (ii) A covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3). (iii) The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.*

Covered entities need to be cognizant of differentiating between best practices versus what the Security Rule requires. Vendor management and supply chain risks are important topics due to the potential they have to introduce new threats and risks to organizations. To the extent that such vendors and service providers are business associates, HIPAA treats them the same as covered entities with respect to Security Rule compliance. Covered entities and business associates are required to obtain written satisfactory assurances from business associates that PHI will be protected. Covered entities and business associates are permitted to require more of their business associates and even include more stringent cybersecurity requirements in a BAA. These requirements would need to be agreed upon by both the covered entity and the business associate.

Table 26. Key activities, descriptions, and sample questions for the Business Associate Contracts or Other Arrangements standard

Key Activities	Description	Sample Questions
1. **Contract Must Provide That Business Associates Will Comply With the Applicable Requirements of the Security Rule**[144] **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.* • Readers may find useful resources in Appendix F, including OCR BAA guidance and templates that include applicable language.	• 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?

[144] 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
2. **Contract Must Provide That the Business Associates Enter Into Contracts With Subcontractors to Ensure the Protection of ePHI** **Implementation Specification (Required)**	• *In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit ePHI on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section.*	• Has the business associate identified all of its subcontractors that will create, receive, maintain, or transmit ePHI? • Has the business associate ensured that contracts in accordance with § 164.314 are in place with its subcontractors identified in the previous question?
3. **Contract Must Provide That Business Associates Will Report Security Incidents** **Implementation Specification (Required)**	• *Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured PHI as required by § 164.410.* • Maintain clear lines of communication between covered entities and business associates regarding the protection of ePHI as per the BAA or contract. • Establish a reporting mechanism and a process for the business associate to use in the event of a security incident or breach.	• Is there a procedure in place for reporting security incidents, including breaches of unsecured PHI by business associates? • Have key business associate staff been identified as points of contact in the event of a security incident or breach? • Does the contract include clear time frames and responsibilities regarding the investigation and reporting of security incidents and breaches?
4. **Other Arrangements** **Implementation Specification (Required)**	• *The covered entity complies with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).*	• 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 that assurances cannot be obtained documented?
5. **Business Associate Contracts With Subcontractors** **Implementation Specification (Required)**	• *The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.*	• Do business associate contracts or other arrangements between the business associate and its subcontractors include appropriate language to comply with paragraphs (a)(2)(i) and (a)(2)(ii) of this section?

5.4.2. Requirements for Group Health Plans (§ 164.314(b))

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.*

Table 27. Key activities, descriptions, and sample questions for the Requirements for Group Health Plans standard

Key Activities	Description	Sample Questions
1. **Amend Plan Documents of the Group Health Plan to Address the Plan Sponsor's Security of ePHI** **Implementation Specification (Required)**	• *Amend the plan documents to incorporate provisions to require the plan sponsor 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 the Group Health Plan to Address Adequate Separation** **Implementation Specification (Required)**	• *Amend the plan documents to incorporate provisions to require the plan sponsor 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 the Group Health Plan to Address the Security of ePHI Supplied to the Plan Sponsors' Agents and Subcontractors** **Implementation Specification (Required)**	• *Amend plan documents to incorporate provisions to require the plan sponsor to ensure that any agent 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?
4. **Amend Plan Documents of Group Health Plans to Address the Reporting of Security Incidents** **Implementation Specification (Required)**	• *Amend plan documents to incorporate provisions to require the plan sponsor to report any security incident of which it becomes aware to the group health plan.*	• Is there a procedure in place for security incident reporting? • Are procedures in place for responding to security incidents?

Key Activities	Description	Sample Questions
	• Establish a specific policy for security incident reporting.[145] • Establish a reporting mechanism and a process for the plan sponsor to use in the event of a security incident.	

[145] See Sec. Security Incident Procedures (§ 164.308(a)(6)), *HIPAA Standard: Security Incident Procedures.*

5.5. Policies and Procedures and Documentation Requirements

5.5.1. 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 or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart*.

Table 28. Key activities, descriptions, and sample questions for the Policies and Procedures standard

Key Activities	Description	Sample Questions

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.
	• Consider the importance of documenting processes and procedures for demonstrating the adequate implementation of recognized security practices.
	• Periodically evaluate written policies and procedures to verify that:[146]
	  ○ 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 regulated entity, its staff, its systems, and its business associates.
		• Are reasonable and appropriate policies and procedures to comply with each of the standards, applicable 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 regulated entity?
		  ○ The regulated entity's technical infrastructure, hardware, and software security capabilities?
		  ○ The costs for security measures?
		  ○ The probability and criticality of potential risks to ePHI?

2. **Update the Documentation of the 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.	• Is a process in place for periodically reevaluating the policies and procedures and updating them as necessary?[147]

[146] See Sec. 5.1.8, *HIPAA Standard: Evaluation.*
[147] See Sec. 5.1.8, *HIPAA Standard: Evaluation.*

		• Should HIPAA documentation be 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?[148]

[148] See Sec. 5.5.2, *HIPAA Standard: Documentation*, and Sec. 5.1.5, *HIPAA Standard: Security Awareness and Training*.

5.5.2. Documentation (§ 164.316(b))

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*.

Table 29. Key activities, descriptions, and sample questions for the Documentation standard

Key Activities	Description	Sample Questions
1. **Draft, Maintain, and Update Required Documentation**	• Document 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 be created specifically for the purpose of demonstrating compliance with the HIPAA Security Rule. • Consider the importance of documenting the processes and procedures for demonstrating the adequate implementation of recognized security practices. • Use feedback from risk assessments and contingency plan tests to help determine when to update documentation.	• Are all required policies and procedures documented? • Should HIPAA Security Rule documentation be maintained by the individual responsible for HIPAA Security Rule implementation? • Should HIPAA Security Rule documentation be updated in response to periodic evaluations, following security incidents, and/or after acquisitions of new technology or new procedures? • Have dates of creation and validity periods been included in all documentation? • Has appropriate management reviewed and approved all documentation? • Are actions, activities, and assessments required by the Security Rule documented as appropriate?
2. **Retain Documentation for at Least Six Years** **Implementation Specification (Required)**	• *Retain 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.*	• Have documentation retention requirements under HIPAA been aligned with the organization's other data retention policies?
3. **Ensure 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 the documentation known to all staff who need to access it? • Is availability of the documentation made known as part of education, training, and awareness activities?[149]

[149] See Sec. 5.1.5, *HIPAA Standard: Security Awareness and Training.*

4. **Update Documentation as Required** **Implementation Specification (Required)**	• *Review documentation periodically and update as needed in response to environmental or operational changes that affect the security of the ePHI.*	• Is there a version control procedure that allows for the verification of the timeliness of policies and procedures, if reasonable and appropriate? • Is there a process for soliciting input on updates of policies and procedures from staff, if reasonable and appropriate? • Are policies and procedures updated in response to environmental or operational changes that affect the security of ePHI? • When were the policies and procedures last updated or reviewed?

References

NIST Special Publications (SPs)

[SP_800-30] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[SP_800-37] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[SP_800-53] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[SP_800-53A] Joint Task Force (2022) Assessing Security and Privacy Controls in Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53Ar5

[SP_800-63B] Grassi PA, Newton EM, Perlner RA, Regenscheid AR, Fenton JL, Burr WE, Richer JP, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) Digital Identity Guidelines: Authentication and Lifecycle Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63B, Includes updates as of March 02, 2020. https://doi.org/10.6028/NIST.SP.800-63B

[SP_800-88] Kissel RL, Regenscheid AR, Scholl MA, Stine KM (2014) Guidelines for Media Sanitization. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-88, Rev. 1. https://doi.org/10.6028/NIST.SP.800-88r1

[SP_800-171] Ross RS, Pillitteri VY, Dempsey KL, Riddle M, Guissanie G (2020) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171, Rev. 2, Includes updates as of January 28, 2021. https://doi.org/10.6028/NIST.SP.800-171r2

NIST Interagency or Internal Reports (NIST IRs)

[IR_8286] Stine KM, Quinn SD, Witte GA, Gardner RK (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. https://doi.org/10.6028/NIST.IR.8286

[IR_8286A] Quinn SD, Ivy N, Barrett MP, Feldman L, Witte GA, Gardner RK (2021) Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management. (National

Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286A. https://doi.org/10.6028/NIST.IR.8286A

Web Sites and Other Resources

[HITRUST] HITRUST Alliance (2022) HITRUST CSF. Available at https://hitrustalliance.net/product-tool/hitrust-csf/

[NIST_CSF] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[NIST_NVD] National Institute of Standards and Technology (2022) National Vulnerability Database. Available at nvd.nist.gov

[NIST_OLIR] National Institute of Standards and Technology (2022) National Online Informative References Program. Available at https://csrc.nist.gov/Projects/olir/

[OMB_A-11] Office of Management and Budget (2021) Preparation, Submission, and Execution of the Budget. (The White House, Washington, DC), OMB Circular A-11, August 6, 2021. Available at https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

[SRA_Tool] The Office of the National Coordinator for Health Information Technology (ONC) and the HHS Office for Civil Rights (OCR) (2022) Security Risk Assessment Tool. Available at https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk- assessment-tool

Legislation and Regulation

[HIPAA] Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. 104-191, https://www.govinfo.gov/app/details/PLAW-104publ191.

[HITECH] Health Information Technology for Economic and Clinical Health (HITECH Act), title XIII of division A and title IV of division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. 111-5, https://www.congress.gov/bill/111th-congress/house-bill/1/text

[OMNIBUS] "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule," Volume 78, Issue 17 (January 25, 2013), https://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf

[Sec_3542] "Definitions," Title 44 U.S. Code, Sec. 3542. 2011 ed. https://www.govinfo.gov/app/details/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapIII-sec3542

[Sec_Rule] 45 CFR Part 160 and Part 164 Subparts A and C. Originally published as: "Health Insurance Reform: Security Standards," Volume 68, Issue 34, 8333 (February 20, 2003), https://www.govinfo.gov/app/details/FR-2003-02-20/03-3877.

Appendix A. List of Symbols, Abbreviations, and Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

API
Application Programming Interface

BAA
Business Associate Agreement

BIA
Business Impact Analysis

BYOD
Bring Your Own Device

CFR
Code of Federal Regulations

CISA
Cybersecurity and Infrastructure Security Agency

CISO
Chief Information Security Officer

COOP
Continuity of Operations

CSF
Cybersecurity Framework

CSP
Cloud Service Provider

CSRC
Computer Security Resource Center

DDoS
Distributed Denial of Service

DoS
Denial of Service

DRM
Derived Relationship Mapping

DHHS
Department of Health and Human Services

EDR
Endpoint Detection and Response

ePHI
Electronic Protected Health Information

ERM
Enterprise Risk Management

FBI
Federal Bureau of Investigation

FDA
Food and Drug Administration

FIPS
Federal Information Processing Standard

GRC
Governance, Risk, and Compliance

HC3
Health Sector Cybersecurity Coordination Center

HDO
Healthcare Delivery Organization

HHS
Department of Health and Human Services

HIC-ISBP
Health Industry Cybersecurity Information Sharing Best Practices

HIC-MISO
Health Industry Cybersecurity Matrix of Information Sharing Organizations

HICP
Health Industry Cybersecurity Practices

HIC-SCRiM
Health Industry Cybersecurity Supply Chain Risk Management

HIC-STAT
Health Industry Cybersecurity – Securing Telehealth and Telemedicine

HIC-TCR
Health Industry Cybersecurity Tactical Crisis Response

HIPAA
Health Insurance Portability and Accountability Act of 1996

HITECH Act
Health Information Technology for Economic and Clinical Health Act

HPH
Healthcare and Public Health

ICT
Information and Communications Technology

IoT
Internet of Things

IPsec
Internet Protocol Security

ISAC

Information Sharing and Analysis Center

IT
Information Technology

ITL
Information Technology Laboratory

MDM
Mobile Device Management

MFA
Multi-Factor Authentication

MOU
Memorandum of Understanding

NICE
National Initiative for Cybersecurity Education

NIST
National Institute of Standards and Technology

NIST IR
NIST Interagency Report

NSA
National Security Agency

OCIO
Office of the Chief Information Officer

OCR
Office for Civil Rights

OIG
Office of the Inspector General

OLIR
Online Informative References

OMB
Office of Management and Budget

ONC
Office of the National Coordinator

PACS
Picture Archiving and Communication System

PHI
Protected Health Information

SSL
Secure Sockets Layer

SME
Subject-Matter Expert

SP
Special Publication

SRA
Security Risk Assessment

TLS
Transport Layer Security

TTP
Tactics, Techniques, and Procedures

UPS
Uninterruptible Power Supply

U.S.
United States

US-CERT
United States Computer Emergency Readiness Team

VPN
Virtual Private Network

Appendix B. Glossary

This appendix provides definitions for terms within this document that are defined principally in the HIPAA Security Rule.

addressable
To meet the addressable implementation specifications, a covered entity or business associate 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 electronic protected health information; and (ii) as applicable to the covered entity or business associate - (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. [Sec. Rule, §164.306(d)(3)]

administrative safeguards
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 or business associate's workforce in relation to the protection of that information. [Sec. Rule, §164.304]

affiliated covered entities
Legally separate covered entities that are affiliated may designate themselves as a single covered entity for the purposes of this part. [Sec. Rule, §164.105(b)]

authentication
The corroboration that a person is the one claimed. [Sec. Rule, §164.304]

availability
The property that data or information is accessible and usable upon demand by an authorized person. [Sec. Rule, §164.304]

business associate
(1) Except as provided in paragraph (4) 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 healthcare arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; 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 healthcare arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected 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 may be a business associate of another covered entity.

(3) *Business associate* includes:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) *Business associate* does not include:

(i) A healthcare provider, with respect to disclosures by a covered entity to the healthcare provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

(iv) A covered entity participating in an organized healthcare arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized healthcare arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized healthcare arrangement by virtue of such activities or services. [Sec. Rule, §160.103]

confidentiality
The property that data or information is not made available or disclosed to unauthorized persons or processes. [Sec. Rule, §164.304]

covered entities
Covered entity means: (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 this subchapter. [Sec. Rule, §160.103]

electronic protected health information (electronic PHI, or ePHI)
Information that comes within paragraphs (1)(i) or (1)(ii) of the definition of protected health information as specified in this section (see "protected health information"). [Sec. Rule, §160.103]

healthcare clearinghouse
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. [Sec. Rule, §160.103]

healthcare provider
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 healthcare in the normal course of business. [Sec. Rule, §160.103]

health information
Any information, including genetic information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual. [Sec. Rule, §160.103]

health plan
An individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(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) A Health Maintenance Organization (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) The Voluntary Prescription Drug Benefit Program under Part D of title XVIII of the Act, 42 U.S.C. 1395w-101 through 1395w-152.

(vii) 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)).

(viii) An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy.

(ix) 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.

(x) The healthcare program for active military personnel under title 10 of the United States Code.

(xi) The veterans' healthcare program under 38 U.S.C. chapter 17.

(xii) The Indian Health Service program under the Indian Healthcare 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 Advantage 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, healthcare; or

(B) Whose principal activity is:

(1) The direct provision of healthcare to persons; or

(2) The making of grants to fund the direct provision of healthcare to persons. [Sec. Rule, §160.103]

hybrid entity
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 healthcare components in accordance with paragraph § 164.105(a)(2)(iii)(D).

implementation specification
Specific requirements or instructions for implementing a standard. [Sec. Rule, §160.103]

individually identifiable health information (IIHI)
Information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare 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. [Sec. Rule, §160.103]

information security
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 non-repudiation 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. [44 U.S.C., Sec. 3542]

information system
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.[150] [Sec. Rule, §164.304]

integrity
The property that data or information have not been altered or destroyed in an unauthorized manner. [Sec. Rule, §164.304]

[150] [SP 800-30] defines "information system" as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."

physical safeguards
Physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion. [Sec. Rule, §164.304]

protected health information (PHI)
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:

(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

(ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);

(iii) In employment records held by a covered entity in its role as employer; and

(iv) Regarding a person who has been deceased for more than 50 years. [Sec. Rule, §160.103]

required
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). [Sec. Rule, §164.306(d)(2)]

standard
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 protected health information. [Sec. Rule, §160.103]

technical safeguards
The technology and the policy and procedures for its use that protect electronic protected health information and control access to it. [Sec. Rule, §164.304]

user
A person or entity with authorized access. [Sec. Rule, §164.304]

Appendix C. Risk Assessment Tables

Section 3 of this publication provides foundational information about risk assessment and an approach that regulated entities may choose to use when assessing risks to ePHI. As part of a risk assessment, regulated entities should identify reasonably anticipated threats that can negatively impact the regulated entity's ability to protect ePHI. Identifying threat sources and threat events may not be easy for regulated entities. The tables in this appendix appear in [SP 800-30] and could be helpful in identifying threat sources and threat events as part of a risk assessment.

Table 30. Taxonomy of threat sources

Type of Threat Source	Description	Characteristics

ADVERSARIAL
• Individual
  ○ Outsider
  ○ Insider
  ○ Trusted Insider
  ○ Privileged Insider
• Group
  ○ Ad hoc
  ○ Established
• Organization
  ○ Competitor
  ○ Supplier
  ○ Partner
  ○ Customer
• Nation-State
	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, Intent, Targeting

ACCIDENTAL • User • Privileged User/Administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.	Range of effects

STRUCTURAL
• Information Technology (IT) Equipment
  ○ Storage
  ○ Processing
  ○ Communications
  ○ Display
  ○ Sensor
  ○ Controller
• Environmental Controls
  ○ Temperature/Humidity Controls
  ○ Power Supply
• Software
  ○ Operating System
  ○ Networking
  ○ General-Purpose Application
  ○ Mission-Specific Application
	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances that exceed expected operating parameters.	Range of effects

Type of Threat Source	Description	Characteristics

ENVIRONMENTAL
• Natural or human-made disaster
  ○ Fire
  ○ Flood/Tsunami
  ○ Windstorm/Tornado
  ○ Hurricane
  ○ Earthquake
  ○ Bombing
  ○ Overrun
• Unusual Natural Event (e.g., sunspots)
• Infrastructure Failure/Outage
  ○ Telecommunications
  ○ Electrical Power
	Natural disasters and failures of critical infrastructures on which the organization depends but which are outside of the control of the organization.
	Note: Natural and human-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities that house mission-critical systems, making those systems unavailable for three weeks).
		Range of effects

Table 31. Representative examples of adversarial threat events

Threat Events (Characterized by Tactics, Techniques, and Procedures [TTPs])	Description
Perform reconnaissance and gather information.	
Perform perimeter network reconnaissance and scanning.	Adversary uses commercial or free software to scan organizational perimeters to obtain a better understanding of the information technology infrastructure and improve the ability to launch successful attacks.
Perform network sniffing of exposed networks.	Adversary with access to exposed wired or wireless data channels used to transmit information uses network sniffing to identify components, resources, and protections.
Gather information using open-source discovery of organizational information.	Adversary mines publicly accessible information to gather information about organizational information systems, business processes, users or personnel, or external relationships that the adversary can subsequently employ in support of an attack.
Perform reconnaissance and surveillance of targeted organizations.	Adversary uses various means (e.g., scanning, physical observation) over time to examine and assess organizations and ascertain points of vulnerability.
Perform malware-directed internal reconnaissance.	Adversary uses malware installed inside the organizational perimeter to identify targets of opportunity. Because the scanning, probing, or observation does not cross the perimeter, it is not detected by externally placed intrusion detection systems.
Craft or create attack tools.	
Craft phishing attacks.	Adversary counterfeits communications from a legitimate or trustworthy source to acquire sensitive information, such as usernames, passwords, or SSNs. Typical attacks occur via email, instant messaging, or comparable means that commonly direct users to websites that appear to be legitimate sites while actually stealing the entered information.
Craft spear phishing attacks.	Adversary employs phishing attacks targeted at high-value targets (e.g., senior leaders, executives).

Threat Events (Characterized by Tactics, Techniques, and Procedures [TTPs])	Description
Craft attacks specifically based on deployed information technology environment.	Adversary develops attacks (e.g., crafts targeted malware) that take advantage of knowledge of the organizational information technology environment.
Create counterfeit or spoof website.	Adversary creates duplicates of legitimate websites. When users visit a counterfeit site, the site can gather information or download malware.
Craft counterfeit certificates.	Adversary counterfeits or compromises a certificate authority so that malware or connections will appear legitimate.
Create and operate false front organizations to inject malicious components into the supply chain.	Adversary creates false front organizations with the appearance of legitimate suppliers in the critical life cycle path that then inject corrupted or malicious information system components into the organizational supply chain.
Deliver, insert, or install malicious capabilities.	
Deliver known malware to internal organizational information systems (e.g., virus via email).	Adversary uses common delivery mechanisms (e.g., email) to install or insert known malware (e.g., malware whose existence is known) into organizational information systems.
Deliver modified malware to internal organizational information systems.	Adversary uses more sophisticated delivery mechanisms than email (e.g., web traffic, instant messaging) to deliver malware and possibly modifications of known malware to gain access to internal organizational information systems.
Deliver targeted malware for control of internal systems and the exfiltration of data.	Adversary installs malware that is specifically designed to take control of internal organizational information systems, identify sensitive information, exfiltrate the information back to the adversary, and conceal these actions.
Deliver malware by providing removable media.	Adversary places removable media (e.g., flash drives) containing malware in locations external to organizational physical perimeters but where employees are likely to find the media (e.g., facilities parking lots, exhibits at conferences attended by employees) and use it on organizational information systems.
Insert untargeted malware into downloadable software and/or into commercial information technology products.	Adversary corrupts or inserts malware into common freeware, shareware, or commercial information technology products. Adversary is not targeting specific organizations but simply looking for entry points into internal organizational information systems. Note that this is particularly a concern for mobile applications.
Insert targeted malware into organizational information systems and information system components.	Adversary inserts malware into organizational information systems and information system components (e.g., commercial information technology products), specifically targeting the hardware, software, and firmware used by organizations (based on knowledge gained via reconnaissance).
Insert specialized malware into organizational information systems based on system configurations.	Adversary inserts specialized, non-detectable malware into organizational information systems based on system configurations, specifically targeting critical information system components based on reconnaissance and placement within organizational information systems.
Insert counterfeit or tampered hardware into the supply chain.	Adversary intercepts hardware from legitimate suppliers. Adversary modifies the hardware or replaces it with faulty or otherwise modified hardware.

Threat Events (Characterized by Tactics, Techniques, and Procedures [TTPs])	Description
Insert tampered critical components into organizational systems.	Adversary replaces critical information system components with modified or corrupted components through the supply chain, a subverted insider, or some combination thereof.
Install general-purpose sniffers on organization-controlled information systems or networks.	Adversary installs sniffing software onto internal organizational information systems or networks.
Install persistent and targeted sniffers on organizational information systems and networks.	Adversary places software designed to collect (i.e., sniff) network traffic over a continuous period of time within internal organizational information systems or networks.
Insert malicious scanning devices (e.g., wireless sniffers) inside facilities.	Adversary uses the postal service or other commercial delivery services to deliver a device to organizational mailrooms that is able to scan wireless communications accessible from within the mailrooms and then wirelessly transmit information back to adversary.
Insert subverted individuals into organizations.	Adversary places individuals within organizations who are willing and able to carry out actions to cause harm to organizational mission or business functions.
Insert subverted individuals into privileged positions in organizations.	Adversary places individuals in privileged positions within organizations who are willing and able to carry out actions to cause harm to organizational mission or business functions. Adversary may target privileged functions to gain access to sensitive information (e.g., user accounts, system files) and may leverage access to one privileged capability to get to another capability.
Exploit and compromise.	
Exploit physical access of authorized staff to gain access to organizational facilities.	Adversary follows ("tailgates") authorized individuals into secure or controlled locations to circumvent physical security checks with the goal of gaining access to facilities.
Exploit poorly configured or unauthorized information systems exposed to the internet.	Adversary gains access through the internet to information systems that are not authorized for internet connectivity or that do not meet organizational configuration requirements.
Exploit split tunneling.	Adversary takes advantage of external organizational or personal information systems (e.g., laptop computers at remote locations) that are simultaneously connected securely to organizational information systems or networks and to non-secure remote connections.
Exploit multi-tenancy in a cloud environment.	Adversary, with processes running in an organizationally used cloud environment, takes advantage of multi-tenancy to observe the behavior of organizational processes, acquire organizational information, or interfere with the timely or correct functioning of organizational processes.
Exploit known vulnerabilities in mobile systems (e.g., laptops, smart phones).	Adversary takes advantage of fact that transportable information systems are outside of the physical protection of organizations and logical protection of corporate firewalls and compromises the systems based on known vulnerabilities to gather information from those systems.
Exploit recently discovered vulnerabilities.	Adversary exploits recently discovered vulnerabilities in organizational information systems in an attempt to compromise the systems before mitigation measures are available or in place.

Threat Events (Characterized by Tactics, Techniques, and Procedures [TTPs])	Description
Exploit vulnerabilities on internal organizational information systems.	Adversary searches for known vulnerabilities in organizational internal information systems and exploits those vulnerabilities.
Exploit vulnerabilities using zero-day attacks.	Adversary employs attacks that exploit as yet unpublicized vulnerabilities. Zero-day attacks are based on adversary insight into the information systems and the applications used by organizations as well as adversary reconnaissance of organizations.
Exploit vulnerabilities in information systems timed with organizational mission or business operations tempo.	Adversary launches attacks on organizations in a time and manner consistent with organizational needs to conduct mission or business operations.
Exploit insecure or incomplete data deletion in a multi-tenant environment.	Adversary obtains unauthorized information due to insecure or incomplete data deletion in a multi-tenant environment (e.g., in a cloud computing environment).
Violate isolation in a multi-tenant environment.	Adversary circumvents or defeats isolation mechanisms in a multi-tenant environment (e.g., in a cloud computing environment) to observe, corrupt, or deny service to hosted services and information or data.
Compromise critical information systems via physical access.	Adversary obtains physical access to organizational information systems and makes modifications.
Compromise information systems or devices used externally and reintroduced into the enterprise.	Adversary installs malware on information systems or devices while the systems/devices are external to organizations in order to subsequently infect organizations when reconnected.
Compromise the software of organizational critical information systems.	Adversary inserts malware or otherwise corrupts critical internal organizational information systems.
Compromise organizational information systems to facilitate exfiltration of data or information.	Adversary implants malware into internal organizational information systems where the malware can identify and exfiltrate valuable information over time.
Compromise mission-critical information.	Adversary compromises the integrity of mission-critical information, thus preventing or impeding the ability of organizations to which information is supplied from carrying out operations.
Compromise the design, manufacturing, and/or distribution of information system components (including hardware, software, and firmware).	Adversary compromises the design, manufacturing, and/or distribution of critical information system components at selected suppliers.
Conduct an attack (i.e., direct or coordinate attack tools or activities).	
Conduct communications interception attacks.	Adversary takes advantage of communications that are either unencrypted or use weak encryption (e.g., encryption containing publicly known flaws), targets those communications, and gains access to the transmitted information and channels.
Conduct wireless jamming attacks.	Adversary takes measures to interfere with wireless communications so as to impede or prevent communications from reaching the intended recipients.
Conduct attacks using unauthorized ports, protocols, and services.	Adversary conducts attacks using ports, protocols, and services for ingress and egress that are not authorized for use by organizations.

Threat Events (Characterized by Tactics, Techniques, and Procedures [TTPs])	Description
Conduct attacks leveraging traffic or data movement allowed across the perimeter.	Adversary makes use of permitted information flows (e.g., email communication, removable storage) to compromise internal information systems, which allows the adversary to obtain and exfiltrate sensitive information through perimeters.
Conduct simple denial-of-service (DoS) attacks.	Adversary attempts to make an internet-accessible resource unavailable to intended users or prevent the resource from functioning efficiently or at all, whether temporarily or indefinitely.
Conduct distributed denial-of-service (DDoS) attacks.	Adversary uses multiple compromised information systems to attack a single target, thereby causing a denial of service for users of the targeted information systems.
Conduct targeted denial-of-service (DoS) attacks.	Adversary conducts DoS attacks to target critical information systems, components, or supporting infrastructures based on adversary knowledge of dependencies.
Conduct physical attacks on organizational facilities.	Adversary conducts a physical attack on organizational facilities (e.g., sets a fire).
Conduct physical attacks on infrastructures that support organizational facilities.	Adversary conducts a physical attack on one or more infrastructures that support organizational facilities (e.g., breaks a water main, cuts a power line).
Conduct cyber-physical attacks on organizational facilities.	Adversary conducts a cyber-physical attack on organizational facilities (e.g., remotely changes heating and/or energy settings).
Conduct data scavenging attacks in a cloud environment.	Adversary obtains data used and then deleted by organizational processes running in a cloud environment.
Conduct brute force login attempts or password guessing attacks.	Adversary attempts to gain access to organizational information systems by random or systematic guessing of passwords, possibly supported by password-cracking utilities.
Conduct non-targeted zero-day attacks.	Adversary employs attacks that exploit as yet unpublicized vulnerabilities. Attacks are not based on any adversary insights into specific vulnerabilities of organizations.
Conduct externally-based session hijacking.	Adversary takes control of (i.e., hijacks) already established, legitimate information system sessions between organizations and external entities (e.g., users connecting from off-site locations).
Conduct internally-based session hijacking.	Adversary places an entity within organizations in order to gain access to organizational information systems or networks for the express purpose of taking control (i.e., hijacking) an already established, legitimate session either between organizations and external entities (e.g., users connecting from remote locations) or between two locations within internal networks.
Conduct externally-based network traffic modification (machine-in-the-middle) attacks.	Adversary, operating outside of organizational systems, intercepts or eavesdrops on sessions between organizational and external systems. Adversary then relays messages between organizational and external systems, making them believe that they are talking directly to each other over a private connection when, in fact, the entire communication is controlled by the adversary. Such attacks are of particular concern for the organizational use of community, hybrid, and public clouds.
Conduct internally-based network traffic modification (man-in-the-middle) attacks.	Adversary intercepts and corrupts data sessions while operating within the organizational infrastructure.

Threat Events (Characterized by Tactics, Techniques, and Procedures [TTPs])	Description
Conduct outsider-based social engineering to obtain information.	Externally placed adversary takes actions (e.g., using email, phone) with the intent of persuading or otherwise tricking individuals within organizations into revealing critical or sensitive information (e.g., personally identifiable information).
Conduct insider-based social engineering to obtain information.	Internally placed adversary takes actions (e.g., using email, phone) so that individuals within organizations reveal critical or sensitive information (e.g., mission information).
Conduct attacks that target and compromise the personal devices of critical employees.	Adversary targets key organizational employees by placing malware on their personally owned information systems and devices (e.g., laptop/notebook computers, personal digital assistants, smart phones). The intent is to take advantage of any instances where employees use personal information systems or devices to handle critical or sensitive information.
Conduct supply chain attacks that target and exploit critical hardware, software, or firmware.	Adversary targets and compromises the operation of software (e.g., through malware injections), firmware, and hardware that performs critical functions for organizations. This is largely accomplished as supply chain attacks on both commercial off-the-shelf and custom information systems and components.
Achieve results (i.e., cause adverse impacts, obtain information).	
Obtain sensitive information by network sniffing external networks.	Adversary with access to exposed wired or wireless data channels that organizations (or organizational personnel) use to transmit information (e.g., kiosks, public wireless networks) intercepts communications.
Obtain sensitive information via exfiltration.	Adversary directs malware on organizational systems to locate and surreptitiously transmit sensitive information.
Cause the degradation or denial of attacker-selected services or capabilities.	Adversary directs malware on organizational systems to impair the correct and timely support of organizational mission and business functions.
Cause the deterioration or destruction of critical information system components and functions.	Adversary destroys or causes the deterioration of critical information system components to impede or eliminate the organizational ability to carry out mission or business functions. Detection of this action is not a concern.
Cause integrity loss by creating, deleting, and/or modifying data on publicly accessible information systems (e.g., web defacement).	Adversary vandalizes or otherwise makes unauthorized changes to organizational websites or data on websites.
Cause integrity loss by polluting or corrupting critical data.	Adversary implants corrupted and incorrect data in critical data, resulting in suboptimal actions or the loss of confidence in organizational data and services.
Cause integrity loss by injecting false but believable data into organizational information systems.	Adversary injects false but believable data into organizational information systems, resulting in suboptimal actions or the loss of confidence in organizational data and services.
Cause the disclosure of critical and/or sensitive information by authorized users.	Adversary induces (e.g., via social engineering) authorized users to inadvertently expose, disclose, or mishandle critical or sensitive information.

Threat Events (Characterized by Tactics, Techniques, and Procedures [TTPs])	Description
Cause unauthorized disclosure and/or unavailability by spilling sensitive information.	Adversary contaminates organizational information systems (including devices and networks) by causing them to handle information of a classification or sensitivity for which they have not been authorized. The information is exposed to individuals who are not authorized access to such information, and the information system, device, or network is unavailable while the spill is investigated and mitigated.
Obtain information by the externally located interception of wireless network traffic.	Adversary intercepts organizational communications over wireless networks (e.g., targets public wireless access or hotel networking connections, drive-by subversion of home or organizational wireless routers).
Obtain unauthorized access.	Adversary with authorized access to organizational information systems gains access to resources that exceed authorization.
Obtain sensitive data or information from publicly accessible information systems.	Adversary scans or mines information on publicly accessible servers and web pages of organizations with the intent of finding sensitive information.
Obtain information by opportunistically stealing or scavenging information systems or components.	Adversary steals information systems or components (e. g., laptop computers or data storage media) that are left unattended outside of the physical perimeters of organizations or scavenges discarded components.
Maintain a presence or set of capabilities.	
Obfuscate adversary actions.	Adversary takes actions to inhibit the effectiveness of the intrusion detection systems or auditing capabilities within organizations.
Adapt cyber attacks based on detailed surveillance.	Adversary adapts their behavior in response to surveillance and organizational security measures.
Coordinate a campaign.	
Coordinate a campaign of multi-staged attacks (e.g., hopping).	Adversary moves the source of malicious commands or actions from one compromised information system to another, making analysis difficult.
Coordinate a campaign that combines internal and external attacks across multiple information systems and information technologies.	Adversary combines attacks that require both a physical presence within organizational facilities and cyber methods to achieve success. The physical attack steps may be as simple as convincing maintenance personnel to leave doors or cabinets open.
Coordinate campaigns across multiple organizations to acquire specific information or achieve a desired outcome.	Adversary does not limit planning to the targeting of one organization. Adversary observes multiple organizations to acquire necessary information on targets of interest.
Coordinate a campaign that spreads attacks across organizational systems from an existing presence.	Adversary uses an existing presence within organizational systems to extend the adversary's span of control to other organizational systems, including organizational infrastructure. Adversary is, thus, in a position to further undermine the organization's ability to carry out mission and business functions.
Coordinate a campaign of continuous, adaptive, and changing cyber attacks based on detailed surveillance.	Adversary attacks continually change in response to surveillance and organizational security measures.
Coordinate cyber attacks using external (outsider), internal (insider), and supply chain (supplier) attack vectors.	Adversary employs continuous, coordinated attacks, potentially using all three attack vectors for the purpose of impeding organizational operations.

Table 32. Representative examples of non-adversarial threat events

Threat Event	Description
Spill sensitive information	An authorized user erroneously contaminates a device, information system, or network by placing on it or sending to it information of a classification or sensitivity that it has not been authorized to handle. The information is exposed to access by unauthorized individuals, and as a result, the device, system, or network is unavailable while the spill is investigated and mitigated.
Mishandling of critical and/or sensitive information by authorized users	An authorized privileged user inadvertently exposes critical or sensitive information.
Incorrect privilege settings	An authorized privileged user or administrator erroneously assigns a user excessive privileges or sets privilege requirements on a resource too low.
Communications contention	Communications performance is degraded due to contention.
Unreadable display	The display is unreadable due to aging equipment.
Earthquake at primary facility	An earthquake of an organization-defined magnitude at the primary facility makes that facility inoperable.
Fire at primary facility	A fire (not due to adversarial activity) at the primary facility makes that facility inoperable.
Fire at backup facility	A fire (not due to adversarial activity) at a backup facility makes that facility inoperable or destroys backups of software, configurations, data, and/or logs.
Flood at primary facility	A flood (not due to adversarial activity) at the primary facility makes that facility inoperable.
Flood at backup facility	A flood (not due to adversarial activity) at a backup facility makes that facility inoperable or destroys backups of software, configurations, data, and/or logs.
Hurricane at primary facility	A hurricane of organization-defined strength at the primary facility makes that facility inoperable.
Hurricane at backup facility	A hurricane of organization-defined strength at a backup facility makes that facility inoperable or destroys backups of software, configurations, data, and/or logs.
Resource depletion	Processing performance is degraded due to resource depletion.
Introduction of vulnerabilities into software products	Due to inherent weaknesses in programming languages and software development environments, errors and vulnerabilities are introduced into commonly used software products.
Disk error	Storage is corrupted due to a disk error.
Pervasive disk error	The aging of a set of devices that were all acquired at the same time and from the same supplier leads to multiple disk errors.
Windstorm or tornado at primary facility	A windstorm or tornado of organization-defined strength at the primary facility makes that facility inoperable.
Windstorm or tornado at backup facility	A windstorm or tornado of organization-defined strength at a backup facility makes that facility inoperable or destroys backups of software, configurations, data, and/or logs.

Appendix D. Security Rule Standards and Implementation Specifications Crosswalk

The tables in Sec. 5 provide key activities, descriptions, and sample questions for each of the Security Rule's standards and implementation specifications and are meant to serve as considerations for a regulated entity when implementing the Security Rule. Some regulated entities may desire more guidance about how to implement the standards and implementation specifications of the Security Rule.

This appendix provides a list of the HIPAA Security Rule [Sec. Rule] standards and implementation specifications within the Administrative (§ 164.308), Physical (§ 164.310), and Technical (§ 164.312) Safeguards sections, as well as the Organizational Requirements (§ 164.314) and Policies and Procedures and Documentation Requirements (§ 164.316). Additionally, this appendix crosswalks or maps the Security Rule standards and implementation specifications to applicable security controls detailed in [SP 800-53], the Cybersecurity Framework [NIST CSF] Subcategories, and NIST publications that are relevant to each Security Rule standard. The key activities, descriptions, and sample questions from the tables in Sec. 5 have also been included to have as much information as possible in one place for readers.

Regulated entities may draw upon these NIST publications and mappings to improve their security posture and assist in achieving compliance with the Security Rule. Regulated entities can reference the listed NIST publications if they need more information about a particular topic, standard, or implementation specification. If the regulated entity utilizes the Cybersecurity Framework, this mapping shows the Subcategory[151] outcomes that align with each of the Security Rule's standards and implementation specifications. The mappings to SP 800-53 can provide information about security controls that can be implemented for a particular standard or implementation specification.

So that the information in this appendix can be more easily kept up to date, the mapping table has been removed from the document and placed online in the NIST Cybersecurity and Privacy Reference Tool (CPRT). Regulated entities should note that the information in the mapping table is informative and should not be considered a complete checklist of requirements that guarantee compliance with the Security Rule.

[151] Note that the mapping to Cybersecurity Framework v1.1 Subcategories was intentionally broad and includes mappings to Subcategories that both directly and indirectly align with standards and implementation specifications of the Security Rule. Once Cybersecurity Framework v2.0 is finalized, this mapping will be updated and may include only those Subcategories that directly align with the standards and implementation specification.

Appendix E. National Online Informative References (OLIR) Program

The mapping in Appendix D lists relevant [NIST CSF] Subcategories and [SP 800-53] security controls for each of the Security Rule's standards and implementation specifications. But what if the regulated entity uses a different framework or controls catalog? Can the regulated entity know which Security Rule standards and implementation specifications align with their chosen framework or controls catalog? The NIST National Online Informative References (OLIR) Program can help regulated entities understand how the Security Rule standards and implementation specifications align with other frameworks and controls catalogs (e.g., the Center for Internet Security [CIS] Critical Security Controls, [HITRUST] CSF), thereby assisting regulated entities in achieving compliance with the Security Rule and improving their cybersecurity posture.

In a general sense, an informative reference (sometimes called a mapping) indicates how one document relates to another document. Within the context of the OLIR Program, an informative reference indicates the relationships between the elements of two documents. The source document, called the Focal Document, is used as the basis for the document comparison. The second document is called the Reference Document. A Focal Document Element or a Reference Document Element is a discrete section, sentence, phrase, or other identifiable piece of content of a document. Traditionally, informative references were published within static NIST documents, like the Cybersecurity Framework. Unfortunately, the informative references often became outdated as the Reference Documents were updated.

The OLIR Program is a NIST effort to help subject matter experts (SMEs) define standardized relationships between elements of their cybersecurity, privacy, and workforce documents (i.e., Reference Documents) and elements of other cybersecurity, privacy, and workforce documents (i.e., Focal Documents), like the Cybersecurity Framework Version 1.1 and SP 800-53r5. By removing the informative references from within NIST documents, the OLIR program scales to accommodate a greater number of informative references while providing a more agile model for updating the relationships between elements of the Reference and Focal Documents.

The OLIR Program provides an online catalog for displaying, sharing, and comparing informative references. **Figure 1** shows some of the existing informative references in the OLIR catalog. These include mappings from the Cybersecurity Framework v1.1 (shown in the column titled "Focal Document") to the CIS Critical Security Controls, Control Objectives for Information and Related Technology (COBIT) 2019, and three versions of the HITRUST CSF (shown in the column titled "Reference Document"), among others. Since there are currently no mappings in the OLIR catalog to the Security Rule as a Reference Document,[152] regulated entities could use the mappings shown in **Fig. 1** to assist in their Security Rule compliance efforts.[153]

[152] There is currently an effort to place the mappings between the Security Rule and Cybersecurity Framework (as shown in Appendix D) and between the Security Rule and SP 800-53 security controls into the OLIR catalog. When Cybersecurity Framework v2.0 is released, it may be a useful effort to update the existing mapping between the Security Rule and the Cybersecurity Framework v1.1 (shown in Appendix D) in the OLIR catalog for the benefit of regulated entities.

[153] Regulated entities that request healthcare information from federal agencies may also need to comply with SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. The OLIR catalog contains a mapping from Cybersecurity Framework v1.1 to SP 800-171 that may benefit regulated entities that need to comply with SP 800-171.

Informative Reference (version)	Reference Document	Date	Focal Document
SECURE-CONTROLS-FRAMEWORK-SCFV2023.2-TO-CSF-V1.1 (1.0.0) (More Details)	Secure-Controls-Framework-SCFv2023.2	2023-07-17	Framework for Improving Critical Infrastructure Cybersecurity
NIST-CSF-TO-NERC-CIP-OLIR-MAPPING (1.0.0) (More Details)	United States Mandatory Standards Subject to Enforcement	2023-07-17	Framework for Improving Critical Infrastructure Cybersecurity
HITRUST-CSF-V9-6-0-TO-NIST-CSF-V1-1 (1.0.0) (More Details)	HITRUST CSF v9.6x	2022-04-19	Framework for Improving Critical Infrastructure Cybersecurity
COBIT 2019 OLIR (1.0.0) (More Details)	COBIT 2019	2020-08-26	Framework for Improving Critical Infrastructure Cybersecurity
TS MITIGATION™ -OPEN (1.0.0) (More Details)	ts mitigation™ - open v1.1	2020-05-11	Framework for Improving Critical Infrastructure Cybersecurity
HITRUST-CSF-V9-3-1-TO-NIST-CSF-V1-1 (1.0.0) (More Details)	HITRUST CSF v9.3.1	2020-03-10	Framework for Improving Critical Infrastructure Cybersecurity
CIS CRITICAL SECURITY CONTROLS (1.0.0) (More Details)	CIS Controls	2019-11-21	Framework for Improving Critical Infrastructure Cybersecurity
HITRUST-CSF-V9-2-TO-NIST-CSF-V1-1 (1.0.0) (More Details)	HITRUST CSF v9.2	2019-11-19	Framework for Improving Critical Infrastructure Cybersecurity
ISF STANDARD OF GOOD PRACTICE FOR INFORMATION SECU (1.0.0) (More Details)	ISF Standard of Good Practice for Information Security 2018	2019-11-14	Framework for Improving Critical Infrastructure Cybersecurity

Fig. 1. Excerpt of informative references in the OLIR catalog

For example, a regulated entity implementing the CIS Critical Security Controls could use the "CIS CRITICAL SECURITY CONTROLS (1.0.0)" (shown in the first column) informative reference in conjunction with the mappings provided in Appendix D. The regulated entity could begin by consulting the mapping in Appendix D to identify the applicable Cybersecurity Framework Subcategories for a standard or implementation specification. Then the regulated entity could use the "CIS CRITICAL SECURITY CONTROLS (1.0.0)" informative reference to locate the applicable CIS critical security controls for each identified Cybersecurity Framework Subcategory. This process would help the regulated entity determine the CIS critical security controls that align with the standards and implementation specifications of the Security Rule.

Another helpful component of the OLIR Program is the Derived Relationship Mapping (DRM) Analysis Tool. A DRM is the result of using the relationships between Reference Documents and a Focal Document to make inferences about relationships between the Reference Documents.

For example, the OLIR catalog contains an informative reference that maps Subcategories of the Cybersecurity Framework to security controls in SP 800-53r5. Another informative reference maps elements of the Cybersecurity Framework to elements in multiple versions of the HITRUST CSF. A DRM can be created that depicts the relationships between the two Reference Documents: SP 800-53r5 and the HITRUST CSF. This DRM can help a regulated entity understand the SP 800-53 security controls that align with the various elements of the HITRUST CSF. These DRMs can be dynamically generated on the OLIR website.

With much of the relationship data already defined by the SME, a user can simply generate a full report between two Reference Documents and export it to a comma-separated values format. The user can sort the reference data by Functions, Categories, Subcategories, Control Families, Security/Privacy Controls, or Security Control Enhancements (depending on the Focal Document selected). The user can then better understand the similarities and differences between the elements and determine which relationships are relevant for their purposes.

Using the mappings in Appendix D, informative references in the OLIR catalog, and the DRM tool, users can determine relationships to elements in a wide variety of other Reference Documents (e.g., controls catalogs, standards, practices) that may help them comply with the Security Rule and improve their organizational cybersecurity posture.

Appendix F. HIPAA Security Rule Resources (Informative)

This appendix lists resources (e.g., guidance, templates, tools) that regulated entities may find useful for achieving compliance with the Security Rule [Sec. Rule] and improving the security posture of their organizations. As with Appendix D, the list has been removed from the document and placed online (as Supplemental Material on the SP 800-66r2 CSRC page) to be more accessible and so that it can be kept up to date.

For ease of use, the resources are organized by topic. This listing is not meant to be exhaustive or prescriptive, nor is there any indication of priority in the listing of resources within a topic. However, there has been an attempt to organize the resources within each topic so that foundational resources (e.g., getting started guides or tools) appear at the beginning of the topic. Regulated entities can consult these resources when they need additional information or guidance about a particular topic. Regulated entities should note that some links may lead to for-cost resources. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or resources are necessarily the best available for the purpose.

Appendix G. Change Log

PubID	Date	Type of Edit	Change	Location
NIST SP 800-66r2	February 2024	Substantive	Updated the content of the Executive Summary to highlight sections of the document.	Executive Summary
NIST SP 800-66r2	February 2024	Substantive	Updated Introduction content.	Section 1
NIST SP 800-66r2	February 2024	Substantive	Updated Section 2 to include a table of Security Rule standards and implementation specifications. Removed previous section 2.2.	Section 2
NIST SP 800-66r2	February 2024	Substantive	Moved Appendix E of Revision 1 to be a separate Section 3 that focuses on Risk Assessment. Updated the Risk Assessment section to align with content from SP 800-30 and the NIST IR 8286 series of documents.	Section 3
NIST SP 800-66r2	February 2024	Substantive	Moved the Risk Management section to Section 4 and updated the content to align with the NIST IR 8286 series of documents.	Section 4
NIST SP 800-66r2	February 2024	Editorial	Updated the section "Considerations When Applying the HIPAA Security Rule" and added Descriptions and Sample Questions.	Section 5
NIST SP 800-66r2	February 2024	Editorial	Moved References from Appendix C to the end of the body to match the updated template. Updated references as needed.	References
NIST SP 800-66r2	February 2024	Editorial	Moved Acronyms from Appendix B to Appendix A and updated as needed.	Appendix A
NIST SP 800-66r2	February 2024	Editorial	Moved Glossary from Appendix A to Appendix B to match the updated template.	Appendix B
NIST SP 800-66r2	February 2024	Substantive	Created Appendix C, including the risk assessment tables that appear in SP 800-30. These are references from Section 3, Risk Assessment.	Appendix C
NIST SP 800-66r2	February 2024	Substantive	Extracted the crosswalk table from Appendix D and moved it online to the NIST Cybersecurity and Privacy Reference Tool for easier reference by readers. Also combined this online table to include the key activities, descriptions, and sample questions from Section 5 to provide more information in one place.	Appendix D

PubID	Date	Type of Edit	Change	Location
NIST SP 800-66r2	February 2024	Substantive	Added Appendix E to introduce the NIST Online Informative Reference (OLIR) Program and its proposed benefits for regulated entities.	Appendix E
NIST SP 800-66r2	February 2024	Substantive	Added Appendix F, HIPAA Security Rule Resources, to include topical listings of resources for the benefit of readers. Extracted this list of resources to be included online for easier reference and update.	Appendix F
NIST SP 800-66r2	February 2024	Substantive	Removed Appendix F, Contingency Planning Guidelines.	Appendix F in Rev 1
NIST SP 800-66r2	February 2024	Substantive	Removed Appendix G, Sample Contingency Plan Template.	Appendix G in Rev 1
NIST SP 800-66r2	February 2024	Substantive	Removed Appendix H, Resources for Secure Remote Use and Access.	Appendix H in Rev 1
NIST SP 800-66r2	February 2024	Substantive	Removed Appendix I, Telework Security Considerations.	Appendix I in Rev 1