NIST Special Publication
NIST SP 800-66r2 ipd

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

A Cybersecurity Resource Guide

Initial Public Draft

Jeffrey A. Marron

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

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

NIST Special Publication
NIST SP 800-66r2 ipd

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

A Cybersecurity Resource Guide

Initial Public Draft

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.ipd

July 2022



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

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.

National Institute of Standards and Technology Special Publication 800-66r2
Natl. Inst. Stand. Technol. Spec. Publ. 800-66r2, 152 pages (July 2022)
Initial Public Draft
CODEN: NSPUE2

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

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment 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.

Public comment period: July 21, 2022 – September 21, 2022

Submit comments on this publication to: sp800-66-comments@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

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

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.

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 protect 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.

Acknowledgments

The author wishes to thank the colleagues who helped update and review this document, specifically Ned Goren, Kevin Stine, Nelson Hastings, Stephen Quinn, Ron Pulivarti, and Isabel Van Wyk from NIST. In addition, special thanks are due to Nick Heesters and Rachel Seeger from the Department of Health and Human Services (HHS) Office for Civil Rights (OCR), who greatly contributed to the document's development. Many thanks are also due to the HHS Office of the Chief Information Officer (OCIO) for their detailed review of the document. The author also gratefully acknowledges the many contributions from the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

Audience

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

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.

Note to Reviewers

NIST would appreciate feedback on the following questions:

- Do you find the overall organization of the document appropriate? Do you have suggestions for improving the document's organization?
- Is it helpful to have the Risk Assessment Guidance and Risk Management Guidance sections sequential? Do you have suggestions for improving these sections and/or making them more useful to regulated entities?
- Are there Key Activities, Descriptions, and/or Sample Questions that should be added to or removed from the tables in Section 5? Are there specific techniques, threats, or topics that need to be added to Section 5 as Key Activities, Descriptions, and/or Sample Questions?
- Does the appendix about the National Online Informative References (OLIR) Program help the reader? Is its purpose clear?
- Is Appendix F helpful in its current format? Are there resources that should be added to or removed from the Appendix? Should Appendix F be reorganized in any way? Does the

annotation of the resources help? Are there additional suggestions for improving Appendix F?

- Are there sections of the publication that would be better extracted from the document and presented elsewhere (e.g., online or as Supplementary Materials hosted on the website)?
- Are there additional topics that should be included in the main body or appendices?

Disclaimer

This publication is intended as general guidance and is provided for informational purposes. This publication is not intended to be, nor should it 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.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to **sp800-66-comments@nist.gov with the Subject: "SP 800-66 Call for Patent Claims."**

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; Other Modifications to the HIPAA Rules [Omnibus Rule][1] and 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 in implementing the Security Rule.

The HIPAA Security Rule specifically focuses on protecting the confidentiality, integrity, and availability of ePHI, as defined in the Security Rule. 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.

The Security Rule is separated into six main sections that each include several standards that a regulated entity must address. 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

[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 includes business associates' subcontractors who have access to ePHI.
[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.

addressable implementation specification is a reasonable and appropriate safeguard for implementation in the regulated entity's environment.

The assessment, analysis, and management of risk to ePHI provides 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 Section 4 provide background information about risk assessment and risk management processes, 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, Section 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 function or 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, as well as the types of activities that a regulated entity may pursue in 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 to applicable security controls detailed in NIST Special Publication (SP) 800-53, Rev. 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, the publication lists a wide variety of resources (e.g., guidance, templates, tools) that regulated entities may find useful in 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 resource topics include:

- Risk Assessment and Risk Management
- Documentation Templates
- Small Regulated Entities
- Telehealth/Telemedicine Guidance
- Mobile Device Security
- Cloud Services
- Ransomware and Phishing
- Education, Training, and Awareness

- Medical Device and Medical Internet of Things (IoT) Security
- Protection of Organizational Resources and Data, including subtopics such as Zero-Trust architecture, digital identities, security of data exchanges, and trustworthy email
- Incident Handling/Response
- Equipment and Data Loss
- Contingency Planning
- Supply Chain
- Information Sharing
- Access Control/Secure Remote Access
- Telework
- Cybersecurity Workforce

Table of Contents

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

1 Introduction **1**

1.1 Purpose and Scope 1

1.2 Applicability 1

1.3 Document Organization 2

1.4 How to Use this Document 3

2 HIPAA Security Rule **4**

2.1 Security Rule Goals and Objectives 4

2.2 Security Rule Organization 5

3 Risk Assessment Guidance **10**

3.1 HIPAA Risk Assessment Requirements 11

3.2 How to Conduct the Risk Assessment 11

3.3 Risk Assessment Results Affect Risk Management 18

4 Risk Management Guidance **20**

4.1 HIPAA Risk Management Requirements 20

4.2 Risk Analysis 20

4.3 Selecting Additional Security Controls to Reduce Risk to ePHI 22

4.4 Documenting Risk Management Activities 23

5 Considerations When Implementing the HIPAA Security Rule **24**

5.1 Administrative Safeguards 26

5.1.1 Security Management Process (§ 164.308(a)(1)) 26

5.1.2 Assigned Security Responsibility (§ 164.308(a)(2)) 30

5.1.3 Workforce Security (§ 164.308(a)(3)) 31

5.1.4 Information Access Management (§ 164.308(a)(4)) 33

5.1.5 Security Awareness and Training (§ 164.308(a)(5)) 35

5.1.6 Security Incident Procedures (§ 164.308(a)(6)) 38

5.1.7 Contingency Plan (§ 164.308(a)(7)) 40

5.1.8 Evaluation (§ 164.308(a)(8)) 43

5.1.9 Business Associate Contracts and Other Arrangements (§ 164.308(b)(1)) 46

5.2 Physical Safeguards 48

316 5.2.1 Facility Access Controls (§ 164.310(a)) 48
317 5.2.2 Workstation Use (§ 164.310(b)) 51
318 5.2.3 Workstation Security (§ 164.310(c)) 53
319 5.2.4 Device and Media Controls (§ 164.310(d)) 54
320 5.3 Technical Safeguards 56
321 5.3.1 Access Control (§ 164.312(a)) 56
322 5.3.2 Audit Controls (§ 164.312(b)) 59
323 5.3.3 Integrity (§ 164.312(c)) 61
324 5.3.4 Person or Entity Authentication (§ 164.312(d)) 63
325 5.3.5 Transmission Security (§ 164.312(e)(1)) 65
326 5.4 Organizational Requirements 67
327 5.4.1 Business Associate Contracts or Other Arrangements (§ 164.314(a)) 67
328 5.4.2 Requirements for Group Health Plans (§ 164.314(b)) 69
329 5.5 Policies and Procedures and Documentation Requirements 70
330 5.5.1 Policies and Procedures (§ 164.316(a)) 70
331 5.5.2 Documentation (§ 164.316(b)) 71
332 **References 73**

333
334 **List of Appendices**

335 **Appendix A— Acronyms 81**
336 **Appendix B— Glossary 84**
337 **Appendix C— Risk Assessment Tables 92**
338 **Appendix D— National Online Informative References (OLIR) Program 104**
339 **Appendix E— Security Rule Standards and Implementation Specifications**
340 **Crosswalk 107**
341 **Appendix F— HIPAA Security Rule Resources (Informative) 128**

342

343 **List of Figures**

344 Figure 1 - Informative References Included in Cybersecurity Framework 104

345

346 **List of Tables**

347 Table 1 - Security Rule Standards and Implementation Specifications 7

Table 2 – Common Threat Sources 13
Table 3 – Assessment Scale for Overall Likelihood 14
Table 4. Security Objectives and Impacts 15
Table 5 - Examples of Adverse Impacts 16
Table 6. Sample Risk-Level Matrix 18
Table 7 - Detailed Risk-Level Matrix 18
Table 8 - Taxonomy of Threat Sources 92
Table 9 - Representative Examples – Adversarial Threat Events 94
Table 10 - Representative Examples – Non-Adversarial Threat Events 102
Table 11 - Catalog Headers and Descriptions 107
Table 12 - Crosswalk of Security Rule to NIST Guidance Documents 108

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 might find useful in implementing the Security Rule.

This publication is intended to be an aid to understanding the HIPAA Security Rule and does not supplement, replace, modify, or supersede the Security Rule itself. Anyone seeking clarifications of the HIPAA Security Rule should contact the 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 800-66, Rev. 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 throughout the world that store, process, or transmit ePHI. While the Security Rule requires regulated entities to protect ePHI, covered entities are required by the Privacy Rule[6] to protect 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 PHI – oral, written, and electronic (to the extent not covered by the Security Rule). This part of the Privacy Rule applies to covered entities, not business associates. However, the business associate agreement (BAA) in place between a covered entity and business associate would cover protections for all PHI. Additionally, business associates are

[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.

directly liable for impermissible uses and disclosures of PHI (i.e., a breach). 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 may diverge significantly. NIST SP 800-66 aims to assist all entities seeking further information on the security safeguards discussed in the HIPAA Security Rule, regardless of the particular structures, methodologies, and approaches used to address its requirements.

The preamble of the Security Rule states that HHS does not rate or endorse the use of industry-developed guidelines and/or models. Organizations that 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 not other provisions adopted or raised by the HIPAA Rules, such as 45 CFR § 164.105. This document also 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 for managing identified risks and achieving 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.
- **References** provides references and related source material.
- **Appendix A – 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.

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

- **Appendix D – National Online Informative References (OLIR) Program** introduces the OLIR program and how it can assist regulated entities in implementing the Security Rule.
- **Appendix E – 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 in implementing the Security Rule.
- **Appendix F – HIPAA Security Rule Resources** provides an annotated, topical listing of additional resources that regulated entities may find useful when implementing the standards and implementation specifications of the Security Rule.

1.4 How to Use this Document

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 protection of ePHI. For that reason, regulated entities may benefit from an initial focus on Section 3 and Section 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 listing of relevant resources, discussions of relevant topics, and a crosswalk to controls and practices that may help in implementing the Security Rule.

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 protect 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.

[8] 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*. 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.

2 HIPAA Security Rule

The HIPAA Security Rule [Sec. Rule] specifically focuses on protecting the confidentiality, integrity, and availability of ePHI as defined in 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 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[9] 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.

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 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
- Ensure compliance with the Security Rule by its workforce.

Regulated entities are reminded of the Security Rule's flexibility of approach. Cybersecurity practices will vary across organizations, depending on levels of technical understanding, financial and human resources, and risk tolerance. This flexibility allows regulated entities to customize how they implement HIPAA's Security Rule requirements. 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:

- **Confidentiality** is "the property that data or information is not made available or disclosed to unauthorized persons or processes."

[9] 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.

- **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

To understand the requirements of the HIPAA Security Rule, it is helpful to be familiar with the basic security terminology it uses to describe the security standards. By understanding the requirements and the terminology in the HIPAA Security Rule, it becomes easier to see which 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.[10] The six sections are listed below.

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 electronic protected health information.
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."
4. **Technical Safeguards** – Defined as the "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.

[10] 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*.

Within the Security Rule's sections are standards and implementation specifications. Each HIPAA Security Rule standard is required. A regulated entity is required to comply with all of the standards of the Security Rule with respect to all ePHI. Many of the standards contain implementation specifications. See Table 1 for a listing of the Security Rule's standards and 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.[11] 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:
    - (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.

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.

Appendix E 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 in implementing the Security Rule.

For general HIPAA Security Rule information, visit the HHS Security Rule website.[12]

[11] For more information on the required analysis used to determine the manner of implementation of an implementation specification, see § 164.306(d) of the HIPAA Security Rule (Security standards – General rules: Flexibility of approach).
[12] See https://www.hhs.gov/hipaa/index.html.

574 **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)

Standard	Sections	Implementation Specifications (R)=Required, (A)=Addressable
		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)
		Emergency Access Procedure (R)
		Automatic Logoff (A)
		Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)

Standard	Sections	Implementation Specifications (R)=Required, (A)=Addressable
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)

575

576

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 protection 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 assessment and an approach that regulated entities may choose to use in assessing risk to ePHI. Regulated entities are free to use another risk assessment methodology[13] that provides a comprehensive assessment of risk to ePHI.

This section incorporates the risk assessment concepts and processes described in the NISTIR 8286 [IR 8286] series (specifically NISTIR 8286A [IR 8286A], *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*); NIST SP 800-30, Rev. 1, *Effective Use of Risk Assessments in Managing Enterprise Risk* [SP 800-30]; and NIST SP 800-37, Rev. 2, *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* refers 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), or
  - Environmental (e.g., power surges and spikes, hazmat contamination, environmental pollution).
- *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.

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

- *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, including vulnerabilities and threats. 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 not be able to exploit this vulnerability. In this example of power surges, recommended security controls could range from installing uninterruptible power supply (UPS) systems, additional fuse boxes, standby generators, or even 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 and risk management:

1. **Risk Analysis (R[14])** – 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)** – 163.308(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 will provide a risk assessment methodology that regulated entities may choose to utilize in accordance with 164.308(a)(1)(ii)(A). Section 4 will provide risk management guidance.

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]. It is expected that

[14] "R" indicates a required implementation specification.

these steps will be customized to most 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, or 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 ePHI leaves the organization. Is ePHI transmitted to external third parties, such as cloud service providers or other service providers?

   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 takes teleworkers and any remote work force into consideration, including any external service providers who may have access to ePHI remotely. 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., medical Internet of Things [IoT]) that can store, process, or transmit ePHI. Modern mobile devices 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. 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[15] depends heavily on the scope of the assessment and the size of the regulated entity.

2. **Identify Realistic Threats.** In this step, the regulated entity identifies the potential threat events and threat sources that are applicable to the regulated entity and its operating environment. The listing of threat events and threat sources should include realistic and probable human and natural incidents that can negatively impact the regulated entity's ability to protect ePHI. Use the information gathered from the preparation step (i.e., where ePHI enters the organization, moves through the organization, is stored within the organization, and leaves the organization) to identify realistic threats to ePHI. Be sure to consider threats to the confidentiality, integrity, and availability of ePHI via phishing, ransomware, or insider threat.

[15] 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 the determination of organizational risk tolerance levels, which are valuable for risk management processes. See [IR 8286A] for more information.

688 **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

689 Regulated entities may make use of various sources[16] when identifying relevant threats.
690 Some of the resources listed in Appendix F may help regulated entities identify common
691 threats relevant to small, medium, and large organizations. Internet searches, vendor
692 information, insurance data, and crime statistics are also viable sources of threat data.
693 Ultimately, regulated entities should identify all threats to ePHI. Examples of some
694 common threat sources are listed in Table 2. Regulated entities can also use Tables 8 to
695 10 in Appendix C as resources for identifying relevant threat events and threat sources.

696 3. **Identify Potential Vulnerabilities and Predisposing Conditions.** For any of the various
697 threats identified above to result in an impactful risk, each needs a vulnerability or
698 predisposing condition that can be exploited. The identification of vulnerabilities or
699 conditions that a threat could use to cause impact is an important component of risk
700 assessment. While it is necessary to review threats and vulnerabilities as unique elements,
701 they are often considered at the same time. Many organizations will consider a given loss
702 scenario and evaluate both. What threat sources might initiate which threat events? What
703 vulnerabilities or predisposing conditions might those threat sources exploit to cause an
704 adverse impact?

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

[16] Regulated entities may benefit from [IR 8286A], specifically Section 2.2.2, when identifying threats to ePHI.

4. **Determine the Likelihood of a Threat Exploiting a Vulnerability.** In this step, 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 to 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 result in 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 exploits a vulnerability. As with likelihood determination, a regulated entity may choose to express this impact in qualitative terms, such as "low," "moderate," and "high" or using 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.

   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 – such as the loss of public confidence, the loss of credibility, or damage to an organization's interest – cannot be measured in specific units but can be qualified or described in terms of "high," "moderate," and "low" impacts, for example. 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 to assist in identifying potential adverse impact and to subsequently assign an impact rating to each 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 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 confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in the loss of public confidence, embarrassment, or legal action against the organization.
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

Security Objective	Impacts
	or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, the violation of integrity may 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 is 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. Loss of system functionality and operational effectiveness, for example, may result in the loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.

769

770 **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 - 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

Type of Impact	Impact
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, 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). A risk-level matrix, such as the samples depicted in Table 6 and Table 7, can be used to 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.

   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.

788 **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

789
790 **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

791 7. **Document the Risk Assessment Results.** Once the risk assessment has been completed
792 (i.e., threat events, threat sources, and vulnerabilities identified; likelihood and impact
793 ratings calculated; and risk levels determined), the results of the risk assessment should
794 be documented. Regulated entities may benefit from documenting the risk assessment
795 results in a risk register.[17] Appendix K of NIST [SP 800-30] provides a sample risk
796 assessment report outline that may prove useful to regulated entities. Other entities may
797 prefer to input the risk assessment results into a governance, risk, and compliance (GRC)
798 or enterprise risk management (ERM) tool. Principally, the regulated entity should
799 document all threat/vulnerability pairs (i.e., a scenario in which an identified threat can
800 exploit a vulnerability) applicable to the organization, the likelihood and impact
801 calculations, and the overall risk to ePHI for the threat/vulnerability pair.

802 ## 3.3 Risk Assessment Results Affect Risk Management

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

[17] 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].

some 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.

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. It cannot identify technical vulnerabilities. It is suggested to pair the SRA tool – or any questionnaire tool – with a methodology that could identify technical vulnerabilities (e.g., vulnerability scanning or a vulnerability management program). Software such as the SRA tool will provide output only as good as the information put into the tool. For that reason, regulated entities should follow 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 with compliance to 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, analysis, and management of risk to ePHI provide the foundation of 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 in managing risk to ePHI. Regulated entities, however, are free to use another risk management methodology[18] that effectively protects 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[19])** – 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)** – 163.308(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 163.308(a)(1)(ii)(B).

4.2 Risk Analysis

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 has been completed and documented, the regulated entity will have a listing of applicable

[18] Regulated entities may benefit from the NISTIR 8286 series for more comprehensive risk management methodologies, including how to integrate ePHI risk management with Enterprise Risk Management (ERM).
[19] "R" indicates a required implementation specification.

threat/vulnerability pairs as well as the overall risk rating of each pair to the confidentiality, integrity, and availability of 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.

Risk Appetite and Risk Tolerance

NISTIR 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, on a broad level, 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 Section 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.

A regulated entity's leadership may indicate that organizational risk tolerance is "Medium" and that all risks to ePHI must be brought within that level or below. Any threat/vulnerability pairs that indicate a threat rating above the organizational risk tolerance will need to be addressed. For example, 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[20] 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?

As an example, a regulated entity's risk assessment may have identified ransomware attacks to pose a high level of risk to ePHI (i.e., High likelihood rating and High impact rating). After implementing two required implementation specifications – 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 two required implementation specifications have helped reduce the impact rating to Low, resulting in an overall risk rating that

[20] 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.

is within organizational risk tolerance. Another regulated entity may have determined during a risk assessment that loss of confidentiality of ePHI during transmission to an external party is an unacceptably high risk (i.e., outside of established risk tolerance). However, the regulated entity has determined that the implemented standards and implementation specifications still do not reduce the risk to levels that are within organizational risk tolerance and that additional controls are needed[21].

This process of risk analysis should be completed for each threat/vulnerability pair to determine whether the implemented standards and implementation specifications have reduced risk to ePHI to levels within the organizational risk tolerance level. Ultimately, the regulated entity's risk analysis processes should inform its decisions regarding the implementation of security measures sufficient to reduce risks to ePHI to levels within organizational risk tolerance. Each regulated entity must document[22] 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. In such a situation, the regulated entity should consider implementing additional security controls[23] to reduce the risk to ePHI to established risk tolerance. Appendix E provides a catalog of the HIPAA Security Rule standards and implementation specifications, mapping each 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, as well as 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 be sure to evaluate all technical and non-technical security controls at all places where ePHI is created, received, maintained, processed, or transmitted. This evaluation should determine whether these additional security measures implemented or planned 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.

---

[21] See Section 4.3 for additional discussion.
[22] Regulated entities should consider documenting these decisions in the risk register or wherever the risk assessment results were documented. See Section 4.4.
[23] It should be noted that not all possible recommended security controls can be implemented to reduce risk. To determine which are required and appropriate for a specific organization, a cost-benefit analysis should be conducted for the proposed recommended controls to demonstrate that the costs of implementing the controls can be justified by the 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.

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 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, the 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, etc. 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. The tables should also 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. Many of these activities, however, 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 specific to its own operations 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 E. The crosswalk lists, for each

Security Rule standard, 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. The descriptions include the types of activities that a regulated entity may pursue in 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 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 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. It is possible that organizations with existing information security programs will have 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 therefore 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.*

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[24] that house ePHI. Be sure to identify mobile devices, medical equipment, and medical 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 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?
2. Conduct Risk Assessment[25] [26] **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.* • A risk assessment methodology is included in Section 3 of this document. • Risk assessment resources are also included in Appendix F.	• Are there any prior risk assessments, audit comments, security requirements, and/or security test results? • Is there intelligence available from agencies, the Office of the Inspector General (OIG), the US-CERT, virus alerts, and/or vendors? • What are the 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?

[24] 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 NISTIR [8286] series of documents for more information.
[25] See Section 3, *Risk Assessment Guidance*.
[26] 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
		• 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[27] **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,[28] that outlines organizational risk appetite and risk tolerance, personnel duties, responsible parties, frequency of risk management, and required documentation. • A risk management methodology is included in Section 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? • 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 IT Systems and Services[29] [30]	• Regulated entities should consider how cloud services and other third-party IT system and service offerings can both	• Will new security controls work with the existing IT architecture?

[27] See Section 164.306 of the HIPAA Security Rule and Section 4, *Risk Management Guidance*.
[28] See NISTIR [8286], which describes a cybersecurity risk management program in the context of enterprise risk management.
[29] See Section 164.306(b) of the HIPAA Security Rule.
[30] 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.

Key Activities	Description	Sample Questions

	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, additional hardware, software, or services may be needed to adequately protect information. Considerations for their selection should include the following:
	  ○ Applicability of the IT solution to the intended environment;
	  ○ The sensitivity of the data;
	  ○ The organization's security policies, procedures, and standards; and
	  ○ Other requirements, such as resources available for operation, maintenance, and training.
		• Have the security requirements of the organization been compared with the security features of existing or proposed hardware and software?
		• Has a cost-benefit analysis been conducted to determine the reasonableness of the investment given the security risks identified?
		• Has a training strategy been developed?[31]

5. Create and Deploy Policies and Procedures[32] [33]	• 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.[34] • Create procedures to be followed to accomplish particular security-related tasks. • Establish a frequency for reviewing policy and procedures	• 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?[35] • 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[36] **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 covered 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 relating to violations of these policies and procedures? • Is there a formal process in place to address system misuse, abuse, and fraudulent activity?

[31] See Section 5.1.5, *HIPAA Standard: Security Awareness and Training*.
[32] See Section 5.5.1, *HIPAA Standard: Policies and Procedures.*
[33] 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.
[34] See Section 5.5.1, *HIPAA Standard: Policies and Procedures* and Section 5.5.2, *HIPAA Standard: Documentation.*
[35] See Section 5.1.7, *HIPAA Standard: Contingency Plan.*
[36] See Section 164.306 of the HIPAA Security Rule.

Key Activities	Description	Sample Questions
		• Have employees been made aware of policies concerning sanctions for inappropriate access, use, and disclosure of ePHI? • Has the need and appropriateness of a tiered structure of sanctions that accounts for the magnitude of harm and possible types of inappropriate disclosures been considered? • How will managers and employees be notified regarding suspect activity?
7. Develop and Deploy the Information System Activity Review Process **Implementation Specification (Required)**	• *Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.* • 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?[37] • 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)?
8. Develop Appropriate Standard Operating Procedures[38]	• Determine the types of audit trail data and monitoring procedures that will be needed to derive exception reports.	• How will exception reports or logs be reviewed? • Where will monitoring reports be filed and maintained?
9. Implement the Information System Activity Review and Audit Process[39]	• 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?

1015

1016

[37] See Section 5.1.2, *HIPAA Standard: Assigned Security Responsibility*.
[38] 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.
[39] 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.*

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.
	• 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.[40] • 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?[41]

[40] See Section 5.5.2, *Standard: Documentation*.
[41] See Section 5.1.5, *Security Awareness and Training*, and Section 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.*

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[42]	• 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.[43]	• 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 staff 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[44]	• Ensure that staff members have the necessary knowledge, skills, and abilities to fulfill particular roles (e.g., positions involving access to and use of sensitive information). • Ensure that these requirements are included as part of the personnel hiring process.	• 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?
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.	• Is there an implementation strategy that supports the designated access authorities? • Are applicants' employment and educational references checked, if reasonable and appropriate?

[42] 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.
[43] See Section 5.5.2, *HIPAA Standard: Documentation.*
[44] 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
	• Implement a procedure for obtaining clearance from appropriate offices or individuals where access is provided or terminated.	• 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?
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[45] (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 an employee leaves (e.g., return of all access devices, deactivation of logon accounts [including remote access], and delivery of any needed data solely under the employee'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?

1026

1027

[45] See Section 5.3.1, *HIPAA Standard: Access Control*.

5.1.4 Information Access Management (§ 164.308(a)(4))[46]

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

Key Activities	Description	Sample Questions
1. Isolate Healthcare Clearinghouse Functions[47] **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 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. • Consider whether multiple access control methods are needed to protect ePHI according to results of the risk assessment • Determine whether direct access to ePHI will ever be appropriate for individuals external to the organization	• 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?[48] • Are there documented job descriptions that accurately reflect assigned duties and responsibilities and enforce segregation of duties?[49] • Has the organization documented procedures that specify how authorized personnel will be granted access to ePHI? • Does the organization grant remote access to 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?

[46] See also Section 5.2.1, *HIPAA Standard: Facility Access Controls* and Section 5.3.1, *HIPAA Standard: Access Control.*
[47] 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.
[48] See Section 5.3.1, *HIPAA Standard: Access Control.*
[49] See Section 5.1.3, *HIPAA Standard: Workforce Security.*

Key Activities	Description	Sample Questions
	(e.g., business partners or patients seeking access to their own 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 staff 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[50]	• Evaluate the security features of access controls 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 and personnel procedures, maintenance and review of audit trails, identification and authentication of users, and physical access controls.	• Are there policies and procedures related to the security of access controls?[51] If so, are they updated regularly? • Are authentication mechanisms used to verify the identity of those accessing systems protected from inappropriate manipulation?[52] • Does management regularly review the list of access authorizations, including remote access authorizations, to verify that the list is accurate and has not been inappropriately altered?[53]

1031

1032

[50] 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.
[51] See Section 5.5.2, *HIPAA Section: Documentation.*
[52] See Section 5.3.4, *HIPAA Standard: Person or Entity Authentication.*
[53] See Section 5.1.3, *HIPAA Standard: Workforce Security.*

5.1.5 Security Awareness and Training (§ 164.308(a)(5))[54]

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

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 • Conduct a review of 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 staff need training on any particular organization devices (e.g., medical IoT) 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. • Outline in the security awareness and training program the scope of the awareness and training program; the goals; the target audiences; the learning objectives; the deployment methods, evaluation, and measurement techniques; and the frequency of training.	• Is there a procedure in place to ensure that everyone in the organization, including teleworkers and remote personnel, receives security awareness training? • What type of security training is needed to address specific technical topics based on job responsibility? • When should training be scheduled to ensure that compliance deadlines are met? • Has the organization considered the training needs of non-employees (e.g., contractors, interns)?
3. Protection from Malicious Software, Login Monitoring, and Password Management **Implementation Specifications (All Addressable)**	• As reasonable and appropriate, train employees regarding procedures for: - *Guarding against, detecting, and reporting malicious software;* - *Monitoring login attempts and reporting discrepancies; and* - *Creating, changing, and safeguarding passwords.*	• Do employees know the importance of the timely application of system patches to protect against malicious software and the exploitation of vulnerabilities? • Are employees aware that login attempts may be monitored? • Do employees who monitor login attempts know to whom to report discrepancies?

[54] See also Section 5.2.1, *HIPAA Standard: Facility Access Controls*; Section 5.3.1, *HIPAA Standard: Access Control;* and Appendix F *Resources.*

Key Activities	Description	Sample Questions
	• Incorporate information concerning staff members' roles and responsibilities in implementing these implementation specifications into training and awareness efforts.	• Do employees 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 is reasonable and appropriate. • Consider using a variety of media and avenues according to what is appropriate for the organization based on workforce size, location, level of education, etc. • 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 employees received a copy of and do they have ready access to the organization's security procedures and policies?[55] • Do employees know whom to contact and how to handle a security incident?[56] • Do employees understand the consequences of noncompliance with the stated security policies?[57] • Do employees who travel, telework, or work remotely know how to handle physical laptop security issues and information security issues?[58] • Has the regulated entity researched available training resources? • Is dedicated training staff available for the delivery of security training? If not, who will deliver the training? • What is the security training budget?

[55] See Section 5.5.2, *HIPAA Standard: Documentation.*
[56] See Section 5.1.6, *HIPAA Standard: Security Incident Procedures.*
[57] See Section 5.1.1, *HIPAA Standard: Security Management Process.*
[58] See Section 5.2.4, *HIPAA Standard: Device and Media Controls.*

Key Activities	Description	Sample Questions
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 employees received adequate training to fulfill their security responsibilities? • Are there sanctions if employees do not complete 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 employees 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 Training Plan[59]	• Keep the security awareness and training program current. • Solicit trainee feedback to determine if the training and awareness is 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 employees participate. • Implement corrective actions when problems arise.[60]	• Are employee training and professional development programs documented and monitored, if reasonable and appropriate? • How are new employees trained on security? • Are new non-employees (e.g., contractors, interns) trained on security?

1035

1036

[59] Also required under the HIPAA Security Rule § 164.306, General Requirements, Subsection (e), *Maintenance*. See Section 5.1.8, *HIPAA Standard: Evaluation.*
[60] See Section 5.1.1, *HIPAA Standard: Security Management Process.*

5.1.6 Security Incident Procedures (§ 164.308(a)(6))[61]

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

Key Activities	Description	Sample Questions
1. Determine Goals of Incident Response	• Gain an understanding as to what constitutes a true security incident. Under the HIPAA Security Rule, a security incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system (45 CFR § 164.304). • 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?[62]
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 a 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?
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.*	• 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?

[61] See Section 5.2.1, *HIPAA Standard: Facility Access Controls*; Section 5.3.1, *HIPAA Standard: Access Control;* and Appendix F *Resources.*
[62] See Section 5.1.7, *HIPAA Standard: Contingency Plan.*

Key Activities	Description	Sample Questions
	• Ensure that an organizational incident response policy[63] 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. • Update the procedures as required based on changing organizational needs.[64]	• 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 under what conditions information related to a security breach will be disclosed to the media? • Have appropriate (internal and external) persons who should be informed of a security breach been identified and a contact information list prepared? • Has a written incident response plan been developed and provided to the incident response team?
4. Incorporate Post-Incident Analysis into Updates and Revisions	• Measure effectiveness and update security incident response procedures to reflect lessons learned, and identify actions to take that will improve security controls after a security incident. • 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 information was gained? • Do records reflect new contacts and resources identified for responding to an incident? • Does the organization consider whether current procedures were adequate for responding to a particular security incident?

1039

[63] See Section 5.5.1, *HIPAA Standard: Policies and Procedures.*
[64] See Section 5.5.2, *HIPAA Standard: Documentation.*

5.1.7 Contingency Plan (§ 164.308(a)(7))[65]

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

Key Activities	Description	Sample Questions
1. Develop Contingency Planning Policy[66]	• 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. • Resources related to contingency planning are included in Appendix F of this document.	• 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 the failure in one system may negatively impact another one?
2. Conduct an Applications and Data Criticality Analysis[67] **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 determine risks to service availability and time to restore. • 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.	• 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? • Has the organization sufficiently addressed the availability and reliability of these services (e.g., via service level agreements, contracts)?

[65] See Section 5.2.1, *HIPAA Standard: Facility Access Controls*; Section 5.3.1, *HIPAA Standard: Access Control;* and Appendix F *Resources.*
[66] See Section 5.5.1, *HIPAA Standard: Policies and Procedures.*
[67] 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
3. Identify Preventive Measures[68]	• 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 (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[69]	• Finalize the set of contingency procedures that should be invoked for all identified impacts, including emergency mode operation. The strategy must be adaptable to the existing operating environment and address allowable outage times and associated priorities identified in 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 employees? 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, etc.)?
5. Data Backup Plan and Disaster Recovery Plan **Implementation Specifications (Both Required)**	• *Establish and implement procedures to create and maintain retrievable exact copies of ePHI.* • *Establish (and implement as needed) procedures to restore any loss of data.*	• Is there a formal, written contingency plan? Does it address disaster recovery and data backup?[70] • Does the disaster recovery plan address what data is to be restored? • Do data backup procedures exist that include all ePHI? • 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 tests conducted to ensure the integrity of data backups?

[68] 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.

[69] 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.

[70] See Key Activity 5.1.7.1, *Develop Contingency Planning Policy*.

Key Activities	Description	Sample Questions
		• Is at least one copy of the data backup stored offline to protect against corruption due to ransomware or other similar attacks?
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 (vendors, alternative site or service providers) in testing exercises. • Make key decisions regarding how the testing is to occur (tabletop exercise versus staging a real operational scenario, including actual loss of capability). • Decide how to segment the type of testing based on the assessment of business impact and 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? • 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 is the plan to be tested (e.g., annually)? • When should the plan be revised?

1044

1045

5.1.8 Evaluation (§ 164.308(a)(8))[71]

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.*

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[72]	• Develop and document organizational policies and procedures[73] 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. Metrics and/or measurements can assist in tracking progress over time.	• 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? • 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?

[71] See Section 5.2.1, *HIPAA Standard: Facility Access Controls* and Section 5.3.1, *HIPAA Standard: Access Control.*
[72] 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*.
[73] See Section 5.5.1, *HIPAA Standard: Policies and Procedures.*

Key Activities	Description	Sample Questions
	• 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.	• 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. • 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 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 activities such as reviewing organizational policies and procedures, assessing the implementation of security controls, collecting evidence of security control implementation, and performing physical walk throughs.	• 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? • 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?
4. Document Results[74]	• 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.	• Does the process support the development of security recommendations? • In determining how best to display evaluation results, have written reports that highlight key findings and recommendations been considered?

[74] See Section 5.5.2, *HIPAA Standard: Documentation*.

Key Activities	Description	Sample Questions
	• 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.	• 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, and consider the sensitivity of the ePHI controlled by the organization, its size, complexity, and environmental and/or operational changes (e.g., other relevant laws or accreditation requirements). • In addition to periodic 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?

1051

5.1.9 Business Associate Contracts and Other Arrangements (§ 164.308(b)(1))[75]

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.

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 the following: - 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 • Have outsourced functions involving the use of ePHI been considered, such as the following: - Actuarial services - Data storage and /or aggregation

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

Key Activities	Description	Sample Questions
		- Administrative services - Accreditation - Financial services
2. Establish a Process for Measuring Contract Performance and Terminating the Contract if Security Requirements Are Not Being Met[76]	• Maintain clear lines of communication between covered entities and business associates regarding the protection of ePHI as per the BAA or contract. • Establish criteria for measuring contract performance.	• What is the service being performed? • What is the outcome expected? • 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).[77] 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 CE, BA, or both address encryption)?

1064

[76] See Section 5.4.1, *HIPAA Standard: Business Associate Contracts or Other Arrangements.*
[77] See Section 5.4.1, *HIPAA Standard: Business Associate Contracts or Other Arrangements*.

5.2 Physical Safeguards

5.2.1 Facility Access Controls (§ 164.310(a))[78]

HIPAA Standard: *Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.*

Key Activities	Description	Sample Questions
1. Conduct an Analysis of Existing Physical Security Vulnerabilities[79] [80]	• 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?[81] • 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 our environment?[82] • Do normal physical protections exist (e.g., locks on doors, windows, and other means of preventing unauthorized access)?
2. Identify Corrective Measures[83] [84]	• 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?[85] • 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?[86]

[78] See Section 5.3.1, *HIPAA Standard: Access Control.*
[79] This key activity may be performed as part of the risk analysis implementation specification. See Section 5.1.1, *HIPAA Standard: Security Management Process.*
[80] 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.
[81] See Section 5.2.2, *HIPAA Standard: Workstation Use.*
[82] See Section 5.1.7, *HIPAA Standard: Contingency Plan.*
[83] This key activity may be performed as part of the risk management implementation specification. See Section 5.1.1, *HIPAA Standard: Security Management Process.*
[84] 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.
[85] See Section 5.1.2, *HIPAA Standard: Assigned Security Responsibility.*
[86] See Section 5.1.5, *HIPAA Standard: Security Awareness and Training.*

Key Activities	Description	Sample Questions
		• How will decisions and actions be documented?[87] • Is a landlord 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.[88] • Include documentation of the facility inventory, as well as information regarding the physical maintenance records and the history of changes, upgrades, and other modifications. • Identify points of access to the facility and existing security controls.	• Is there an inventory of facilities and existing security practices? • What are the current procedures for securing the facilities (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?[89]
4. Develop Access Control and Validation Procedures **Implementation Specification (Addressable)**	• *Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision.* • Implement procedures to provide facility access to authorized personnel and visitors and exclude unauthorized persons.	• What are the policies and procedures in place for controlling access by staff, contractors, visitors, and probationary employees? • Do the procedures identify individuals, roles, or job functions that are authorized to access software programs for testing and revision? • How many access points exist in each facility? Is there an inventory? • Is monitoring equipment necessary? • Is there 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, unit, etc.?

[87] See Section 5.5.2, *HIPAA Standard: Documentation.*
[88] 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.
[89] See Section 5.1.7, *HIPAA Standard: Contingency Plan.*

Key Activities	Description	Sample Questions
		• Will the contingency plan be appropriate in the event of all types of potential disasters (e.g., fire, flood, earthquake, etc.)?
6. Maintain Maintenance Records[90] **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?

1069

[90] See Section 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.*

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, such as medical equipment, medical IoT devices, tablets, smart phones, etc. • 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. • What is the proper function and manner by which specific workstations or classes of workstations are permitted to access ePHI (e.g., what applications permitting access to ePHI are allowed on workstations used by a hospital's customer service call center or by 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[91]	• Ensure that any risks associated with a device's surroundings are known and analyzed for possible negative impacts.	• 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?

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

	• 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.	• Is viewing by unauthorized individuals restricted or limited at these devices? • Do changes need to be made in the space configuration? • Do employees understand the security requirements for the data they use in their day-to-day jobs?

1074

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.*

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, such as medical equipment, medical IoT devices, tablets, smart phones, etc. • 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 Risk Associated with Each Type of Access[92]	• 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, or 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 making modifications to 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) - Screen lock - 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 physical safeguards implemented for all devices that access ePHI to restrict access to authorized users? • What safeguards are in place,(e.g., locked doors, screen barriers, cameras, guards)?[93] • Are additional physical safeguards needed to protect devices with ePHI? • Do any devices need to be relocated to enhance physical security? • Have employees been trained on security?[94] • 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?

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

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 itself. • Ensure that ePHI is properly destroyed and cannot be recreated.	• What ePHI is created, stored, processed, and transmitted by the organization, and on what media is it located? • Is data stored on removable, reusable media (e.g., flash drives)? • 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?
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 use. • 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 (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 employees appropriately trained on the security risks to ePHI when reusing software and hardware?[95]
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. • Ensure that an individual is responsible for and records the receipt and removal of hardware and software with ePHI.	• Is a process implemented for maintaining a record of the movements of and persons responsible for hardware and electronic media containing ePHI? • Where is data stored (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?

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

Key Activities	Description	Sample Questions
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 protect the integrity of ePHI during equipment relocation.	• Is a process implemented for creating a retrievable, exact copy of ePHI when needed and before the movement of equipment? • Are backup files maintained offsite to ensure data availability in the event that data is lost while transporting or moving electronic media containing ePHI? • If data were to be unavailable while media are transported or moved for a period of time, what would the business impact be?

1081

1082

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).*

Key Activities	Description	Sample Questions
1. Analyze Workloads and Operations to Identify the Access Needs of All Users[96]	• Identify an approach[97] for access control. • Consider all applications and systems containing ePHI that should be available only to authorized users, processes, and services. • Integrate these activities into the access granting and management process.[98]	• Have all applications and systems with ePHI been identified? • What user roles are defined for those applications and systems? • Is access to systems containing 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)?
3. Ensure that All System Users Have Been Assigned a Unique Identifier[99]	• *Assign a unique name and/or number for identifying and tracking user identity.* • Ensure that system activity can be traced to a specific user.	• How should the identifier be established (e.g., length and content)? • Should the identifier be self-selected, organizationally selected, or randomly generated?

[96] See Section 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 process detailed in the Information Access Management standard.
[97] Consider how Zero Trust Architecture principals can aid in the organization's approach to access control. See Appendix F, *HIPAA Security Rule Resources* for more information.
[98] See Section 5.1.4, *HIPAA Standard: Information Access Management.*
[99] See Appendix F, *HIPAA Security Rule Resources* for information and resources related to Identity Management.

Key Activities	Description	Sample Questions
Implementation Specification (Required)	• Ensure that the necessary data is available in the system logs to support audit and other related business functions.[100]	• Can the unique user identifier be used to track user access to ePHI?
4. Develop Access Control Policy[101] and Procedures	• Establish a formal policy for access control that will guide the development of procedures.[102] • Specify requirements for access control that are both feasible and cost-effective for implementation.[103]	• 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?[104] • Will user training be needed to implement access control procedures?
6. Review and Update Access for Users and Processes	• Enforce policy and procedures as a matter of ongoing operations.[105] • Determine whether any changes are needed for access control mechanisms. • Ensure 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:[106] - Initial access - Increased access - Access to different systems or applications than those they currently have	• Have new employees/users been given proper instructions for protecting data and systems?[107] • What are the procedures for new employee/user access to data and systems?[108] • Are there procedures for reviewing and, if appropriate, modifying access authorizations for existing users, services, and processes?[109] • 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 in reviewing the access needs of users and processes?
7. Establish an Emergency Access Procedure	• *Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.*	• Are there policies and procedures in place to provide appropriate access to ePHI in emergency situations?

[100] See Section 5.3.2, *HIPAA Standard: Audit Controls.*
[101] See Section 5.1.4, *HIPAA Standard: Information Access Management.*
[102] See Section 5.1.4, *HIPAA Standard: Information Access Management.*
[103] See Section 5.1.1, *HIPAA Standard: Security Management Process.*
[104] See Section 5.1.5, *HIPAA Standard: Security Awareness and Training.*
[105] See Section 5.1.4, *HIPAA Standard: Information Access Management.*
[106] See Section 5.1.4, *HIPAA Standard: Information Access Management.*
[107] See Section 5.1.5, *HIPAA Standard: Security Awareness and Training.*
[108] See Section 5.1.4, *HIPAA Standard: Information Access Management.*
[109] See Section 5.1.4, *HIPAA Standard: Information Access Management.*

Key Activities	Description	Sample Questions
Implementation Specification (Required)	• Identify a method of supporting continuity of operations should the normal access procedures be disabled or unavailable due to system problems.	• When should the emergency access procedure be activated? • Who is authorized to make the decision?[110] • Who has assigned roles in the process?[111] • Will systems automatically default to settings and functionalities that will enable the emergency access procedure or will the mode be activated by the system administrator or other authorized individual?
8. Automatic Logoff and Encryption and Decryption **Implementation Specifications (Both Addressable)**	• Consider whether the addressable implementation specifications of this standard are reasonable and appropriate: - *Implement electronic procedures that terminate an electronic session after a predetermined period of inactivity.* - *Implement a mechanism to encrypt and decrypt ePHI.*	• Are automatic logoff features available for any of the regulated entity's operating systems or other major applications? • If applications have been created or developed in-house, is it reasonable and appropriate to modify them to feature automatic logoff capability? • What period of inactivity prior to automatic logoff is reasonable and appropriate for the 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")? • 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[112]	• 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 staff 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?

1088

[110] See Section 5.1.7, *HIPAA Standard: Contingency Plan.*
[111] See Section 5.1.7, *HIPAA Standard: Contingency Plan.*
[112] See Section 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.*

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.[113] • 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?[114] • What systems, applications, or processes make ePHI vulnerable to unauthorized or inappropriate tampering, uses, or disclosures?[115] • What activities will be audited (e.g., creation of ePHI, accessing ePHI, modifying ePHI, transmission of ePHI, and/or deleting of files or records containing 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?[116] • Where will audit information reside (i.e., separate server)?
4. Develop Appropriate Standard Operating Procedures[117]	• Determine the types of audit trail data and monitoring procedures that will be needed to derive exception reports. • Determine the frequency of audit log review 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?

[113] See Section 5.1.1, *HIPAA Standard: Security Management Process* and Key Activity 5.1.1.7, *Develop and Deploy the Information System Activity Review Process.*
[114] See Section 5.1.1, *HIPAA Standard: Security Management Process* and Key Activity 5.1.1.2, *Conduct Risk Assessment.*
[115] See Section 5.1.1, *HIPAA Standard: Security Management Process* and Key Activity 5.1.1.2, *Conduct Risk Assessment.*
[116] See Section 5.1.1, *HIPAA Standard: Security Management Process* and Key Activity 5.1.1.6, *Develop and Implement a Sanction Policy*.
[117] See Section 5.1.1, *HIPAA Standard: Security Management Process* and Key Activity 5.1.1.7, *Develop and Deploy the Information system Activity Review Process*.

Key Activities	Description	Sample Questions
		• 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?[118] • How will managers and employees be notified, when appropriate, regarding suspect activity?
5. Implement the Audit/System Activity Review Process[119]	• 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?

1092

[118] See Section 5.1.1, *HIPAA Standard: Security Management Process* and Key Activity 5.1.1.6, *Develop and Implement a Sanction Policy*.
[119] See Section 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.*

Key Activities	Description	Sample Questions
1. Identify All Users Who Have Been Authorized to Access ePHI[120]	• 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?[121] • Is there a sound basis for why they need the access?[122] • Have they been trained on how to use the information?[123] • Is there an audit trail established for all accesses to the information?[124]
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, disgruntled employees, business competitors).[125] • Conduct this activity as part of a risk analysis.[126]	• What are likely sources that could jeopardize information integrity?[127] • What can be done to protect the integrity of the information when it is residing in a system (at rest)? • What procedures and policies can be established to decrease or eliminate alteration of the information during transmission?[128]
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?
4. Implement Procedures to Address These Requirements	• Identify and implement methods that will be used to protect ePHI from unauthorized modification.	• Are current audit, logging, and access control techniques sufficient to address the integrity of ePHI?

[120] See Section 5.1.3, *HIPAA Standard: Workforce Security,* Section 5.3.1, *HIPAA Standard: Access Control*, and Section 5.5.1, *HIPAA Standard: Policies and Procedures.*
[121] See Section 5.1.3, *HIPAA Standard: Workforce Security* and Section 5.3.1, *HIPAA Standard: Access Control.*
[122] See Section 5.1.3, *HIPAA Standard: Workforce Security.*
[123] See Section 5.1.5, *HIPAA Standard: Security Awareness and Training.*
[124] See Section 5.3.2, *HIPAA Standard: Audit Controls.*
[125] See Section 5.1.1, *HIPAA Standard: Security Management Process.*
[126] See Section 5.1.1, *HIPAA Standard: Security Management Process.*
[127] See Section 5.1.1, *HIPAA Standard: Security Management Process.*
[128] See Section 5.1.1, *HIPAA Standard: Security Management Process* and Section 5.3.5, *HIPAA Standard: Transmission Security.*

Key Activities	Description	Sample Questions
	• Identify and implement tools and techniques to be developed or procured that support the assurance of integrity.	• 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?
6. Establish a Monitoring Process to Assess How the Implemented Process is Working	• Review existing processes to determine whether objectives are being addressed.[129] • Continually reassess integrity processes as technology and operational environments change to determine whether they need to be revised.[130]	• Are there reported instances of information integrity problems, and have they decreased since integrity procedures have been implemented?[131] • Does the process, as implemented, provide a higher level of assurance that information integrity is being maintained?

1096

[129] See Section 5.1.8, *HIPAA Standard: Evaluation.*
[130] See Section 5.1.8, *HIPAA Standard: Evaluation.*
[131] See Section 5.1.6, *HIPAA Standard: Security Incident Procedures.*

5.3.4 Person or Entity Authentication (§ 164.312(d))[132]

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

Key Activities	Description	Sample Questions
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 authentication (and that should require authentication if not currently required). 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 our 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 multi-factor authentication 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, etc.) 3. Some type of biometric identification that a person provides, such as a fingerprint • Multi-factor authentication (MFA) utilizes two or more of the above approaches to enforce stronger authentication. • Consider implementing multi-factor authentication solutions 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? • Has the organization considered MFA for access to ePHI that poses high risk (e.g., remote access, access to privileged functions)? • Is outside vendor support required to implement the process?

[132] See also Section 5.3.1, *HIPAA Standard: Access Control*; Section 5.3.2, *HIPAA Standard: Audit Controls*; and NIST [SP 800-63B], *Digital Identity Guidelines: Authentication and Lifecycle Management*

Key Activities	Description	Sample Questions
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 into 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[133] 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, etc.)?

1100

1101

[133] 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.*

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).[134] • Identify scenarios and pathways that may put ePHI at a high level of risk.	• Have all pathways been identified by which ePHI will be transmitted? • Has the 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?[135] • Are there trained staff members to monitor transmissions?
2. Develop and Implement Transmission Security Policy and Procedures	• Establish a formal (written) set of requirements for transmitting ePHI. • Identify methods of transmission that will be used to safeguard ePHI. • Identify tools and techniques that will be used to support the transmission security policy. • Implement procedures for transmitting ePHI using hardware and/or software, if needed.	• Have the requirements been discussed and agreed to by identified key personnel involved in transmitting ePHI? • Has a written policy been developed and communicated to system users?
3. Implement Integrity Controls **Implementation Specification (Addressable)**	• *Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.*	• What 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?

[134] See Section 5.1.7, *HIPAA Standard: Contingency Plan* and Section 5.1.1, *HIPAA Standard: Security Management Process.*
[135] See Section 5.1.1, *HIPAA Standard: Security Management Process.*

Key Activities	Description	Sample Questions
		• 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 in a manner to disallow negotiation to a level of encryption that would inadequately protect electronic transmissions of ePHI? • Does the covered entity have the appropriate staff to maintain a process for encrypting ePHI during transmission? • Are staff members skilled in the use of encryption?

1105

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.

Key Activities	Description	Sample Questions
1. Contract Must Provide that Business Associates Will Comply with the Applicable Requirements of the Security Rule[136] **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?

[136] 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 the point 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?

1121

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.*

Key Activities	Description	Sample Questions
1. Amend Plan Documents of Group Health Plan to Address 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 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 Group Health Plan to Address Security of ePHI Supplied to Plan Sponsors' Agents and Subcontractors **Implementation Specification (Required)**	• *Amend plan documents to incorporate provisions to require the plan sponsor to ensure that any agent 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 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.* • Establish specific policy for security incident reporting.[137] • Establish a reporting mechanism and a process for the plan sponsor to use in the event of a security incident.	• Is there a procedure in place for security incident reporting? • Are procedures in place for responding to security incidents?

[137] See Section 5.1.6, *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.*

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:[138] - 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 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?[139] • 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?[140]

[138] See Section 5.1.8, *HIPAA Standard: Evaluation.*
[139] See Section 5.1.8, *HIPAA Standard: Evaluation.*
[140] See Section 5.5.2, *HIPAA Standard: Documentation* and Section 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.*

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?
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?[141]
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 into 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?

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

		• When were the policies and procedures last updated or reviewed?

1138

References

NIST Federal Information Processing Standards (FIPS) Publications

[FIPS 140-3] National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3

[FIPS 199] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

[FIPS 200] National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200

NIST Special Publications (SPs)

[SP 800-12] Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1. https://doi.org/10.6028/NIST.SP.800-12r1

[SP 800-16] deZafra DE, Pitcher SI, Tressler JD, Ippolito JB (1998) Information Technology Security Training Requirements: A Role- and Performance-Based Model. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-16. https://doi.org/10.6028/NIST.SP.800-16

[SP 800-18] Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-18, Rev. 1. https://doi.org/10.6028/NIST.SP.800-18r1

[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 800-34] Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency Planning Guide for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-34, Rev. 1, Includes updates as of November 11, 2010. https://doi.org/10.6028/NIST.SP.800-34r1

[SP 800-35] Grance T, Hash J, Stevens M, O'Neal K, Bartol N (2003) Guide to Information Technology Security Services. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-35. https://doi.org/10.6028/NIST.SP.800-35

[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 800-39] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[SP 800-41] Scarfone KA, Hoffman P (2009) Guidelines on Firewalls and Firewall Policy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-41, Rev. 1. https://doi.org/10.6028/NIST.SP.800-41r1

[SP 800-45] Tracy MC, Jansen W, Scarfone KA, Butterfield J (2007) Guidelines on Electronic Mail Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-45, Version 2. https://doi.org/10.6028/NIST.SP.800-45ver2

[SP 800-46] Souppaya MP, Scarfone KA (2016) Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-46, Rev. 2. https://doi.org/10.6028/NIST.SP.800-46r2

[SP 800-47] Dempsey KL, Pillitteri VY, Regenscheid AR (2021) Managing the Security of Information Exchanges. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-47, Rev. 1. https://doi.org/10.6028/NIST.SP.800-47r1

[SP 800-50] Wilson M, Hash J (2003) Building an Information Technology Security Awareness and Training Program. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-50. https://doi.org/10.6028/NIST.SP.800-50

[SP 800-52] McKay KA, Cooper DA (2019) Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-52, Rev. 2. https://doi.org/10.6028/NIST.SP.800-52r2

[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 800-55] Chew E, Swanson MA, Stine KM, Bartol N, Brown A, Robinson W (2008) Performance Measurement Guide for Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-55, Rev. 1. https://doi.org/10.6028/NIST.SP.800-55r1

[SP 800-58] Kuhn DR, Walsh TJ, Fries S (2005) Security Considerations for Voice Over IP Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-58. https://doi.org/10.6028/NIST.SP.800-58

[SP 800-60] Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v2r1

[SP 800-61] Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer Security Incident Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61, Rev. 2. https://doi.org/10.6028/NIST.SP.800-61r2

[SP 800-63-3] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, Includes updates as of March 02, 2020. https://doi.org/10.6028/NIST.SP.800-63-3

[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 800-77] Barker EB, Dang QH, Frankel SE, Scarfone KA, Wouters P (2020) Guide to IPsec VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-77, Rev. 1. https://doi.org/10.6028/NIST.SP.800-77r1

[SP 800-81] Chandramouli R, Rose SW (2013) Secure Domain Name System (DNS) Deployment Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-81-2.

https://doi.org/10.6028/NIST.SP.800-81-2

[SP 800-83] Souppaya MP, Scarfone KA (2013) Guide to Malware Incident Prevention and Handling for Desktops and Laptops. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-83, Rev. 1. https://doi.org/10.6028/NIST.SP.800-83r1

[SP 800-84] Grance T, Nolan T, Burke K, Dudley R, White G, Good T (2006) Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-84. https://doi.org/10.6028/NIST.SP.800-84

[SP 800-86] Kent K, Chevalier S, Grance T, Dang H (2006) Guide to Integrating Forensic Techniques into Incident Response. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-86. https://doi.org/10.6028/NIST.SP.800-86

[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 800-92] Kent K, Souppaya MP (2006) Guide to Computer Security Log Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-92. https://doi.org/10.6028/NIST.SP.800-92

[SP 800-94] Scarfone KA, Mell PM (2007) Guide to Intrusion Detection and Prevention Systems (IDPS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-94. https://doi.org/10.6028/NIST.SP.800-94

[SP 800-100] Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007. https://doi.org/10.6028/NIST.SP.800-100

[SP 800-106] Dang QH (2009) Randomized Hashing for Digital Signatures. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-106. https://doi.org/10.6028/NIST.SP.800-106

[SP 800-107] Dang QH (2012) Recommendation for Applications Using Approved Hash Algorithms. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-107, Rev. 1. https://doi.org/10.6028/NIST.SP.800-107r1

[SP 800-113] Frankel SE, Hoffman P, Orebaugh AD, Park R (2008) Guide to SSL VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-113. https://doi.org/10.6028/NIST.SP.800-113

[SP 800-114] Souppaya MP, Scarfone KA (2016) User's Guide to Telework and Bring Your Own Device (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-114, Rev. 1. https://doi.org/10.6028/NIST.SP.800-114r1

[SP 800-115] Scarfone KA, Souppaya MP, Cody A, Orebaugh AD (2008) Technical Guide to Information Security Testing and Assessment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-115. https://doi.org/10.6028/NIST.SP.800-115

[SP 800-124] Souppaya MP, Scarfone KA (2013) Guidelines for Managing the Security of Mobile Devices in the Enterprise. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-124, Rev. 1. https://doi.org/10.6028/NIST.SP.800-124r1

[SP 800-144] Jansen W, Grance T (2011) Guidelines on Security and Privacy in Public Cloud Computing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-144. https://doi.org/10.6028/NIST.SP.800-144

[SP 800-146] Badger ML, Grance T, Patt-Corner R, Voas JM (2012) Cloud Computing Synopsis and Recommendations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-146. https://doi.org/10.6028/NIST.SP.800-146

[SP 800-150] Johnson CS, Waltermire DA, Badger ML, Skorupka C, Snyder J (2016) Guide to Cyber Threat Information Sharing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-150. https://doi.org/10.6028/NIST.SP.800-150

[SP 800-161] Boyens JM, Smith AM, Bartol N, Winkler K, Holbrook A, Fallon M (2022) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161r1. https://doi.org/10.6028/NIST.SP.800-161r1

[SP 800-177] Rose SW, Nightingale S, Garfinkel SL, Chandramouli R (2019) Trustworthy Email. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-177, Rev. 1. https://doi.org/10.6028/NIST.SP.800-177r1

[SP 800-184] Bartock MJ, Scarfone KA, Smith MC, Witte GA, Cichonski JA, Souppaya MP (2016) Guide for Cybersecurity Event Recovery. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-184. https://doi.org/10.6028/NIST.SP.800-184

[SP 800-207] Rose SW, Borchert O, Mitchell S, Connelly S (2020) Zero Trust Architecture. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-207. https://doi.org/10.6028/NIST.SP.800-207

[SP 800-210] Hu VC, Iorga M, Bao W, Li A, Li Q, Gouglidis A (2020) General Access Control Guidance for Cloud Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-210. https://doi.org/10.6028/NIST.SP.800-210

[SP 1271] Mahn A, Topper D, Quinn SD, Marron JA (2021) Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1271. https://doi.org/10.6028/NIST.SP.1271

NIST Interagency Reports (NISTIRs)

[IR 7621] Paulsen C, Toth PR (2016) Small Business Information Security: The Fundamentals. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7621, Rev. 1. https://doi.org/10.6028/NIST.IR.7621r1

[IR 8228] Boeckl KR, Fagan MJ, Fisher WM, Lefkovitz NB, Megas KN, Nadeau EM, Piccarreta BM, Gabel O'Rourke D, Scarfone KA (2019) Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8228. https://doi.org/10.6028/NIST.IR.8228

[IR 8259] Fagan MJ, Megas KN, Scarfone KA, Smith M (2020) Foundational Cybersecurity Activities for IoT Device Manufacturers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259. https://doi.org/10.6028/NIST.IR.8259

[IR 8259A] Fagan MJ, Megas KN, Scarfone KA, Smith M (2020) IoT Device Cybersecurity Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259A. https://doi.org/10.6028/NIST.IR.8259A

[IR 8259B] Fagan MJ, Marron JA, Brady KG, Jr., Cuthill BB, Megas K, Herold R (2021) IoT Non-Technical Supporting Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259B. https://doi.org/10.6028/NIST.IR.8259B

[IR 8276] Boyens J, Paulsen C, Bartol N, Winkler K, Gimbi J (2021) Key Practices in Cyber Supply Chain Risk Management: Observations from Industry. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8276. https://doi.org/10.6028/NIST.IR.8276

[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/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/114/plaws/publ255/PLAW-114publ255.pdf.

[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—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 Mappings
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	Multifactor Authentication
MOU	Memorandum of Understanding
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NISTIR	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

1415

Appendix B—Glossary

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

addressable [Sec. Rule, §164.306(d)(3)]	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.
administrative safeguards [Sec. Rule, §164.304]	Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.
affiliated covered entities [Sec. Rule, §164.105(b)]	Legally separate covered entities that are affiliated may designate themselves as a single covered entity for the purposes of this part.
authentication [Sec. Rule, §164.304]	The corroboration that a person is the one claimed.
availability [Sec. Rule, §164.304]	The property that data or information is accessible and usable upon demand by an authorized person.
business associate [Sec. Rule, §160.103]	(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.
confidentiality [Sec. Rule, §164.304]	The property that data or information is not made available or disclosed to unauthorized persons or processes.
covered entities [Sec. Rule, §160.103]	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.
electronic protected health information (electronic PHI, or ePHI) [Sec. Rule, §160.103]	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").
healthcare clearinghouse [Sec. Rule, §160.103]	A public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions: (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction. (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.
healthcare provider [Sec. Rule, §160.103]	A provider of services (as defined in section 1861(u) of the Social Security Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Social Security Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for healthcare in the normal course of business.
health information	Any information, including genetic information, whether oral

[Sec. Rule, §160.103]

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.

health plan
[Sec. Rule, §160.103]

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) An HMO, as defined in this section.

(iv) Part A or Part B of the Medicare program under title XVIII of the Social Security Act.

(v) The Medicaid program under title XIX of the Social Security Act, 42 U.S.C. 1396, et seq.

(vi) 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.

hybrid entity
[Sec. Rule, §164.103]

A single legal entity:

(1) That is a covered entity;

(2) Whose business activities include both covered and non-

	covered functions; and (3) That designates healthcare components in accordance with paragraph § 164.105(a)(2)(iii)(D).
implementation specification [Sec. Rule, §160.103]	Specific requirements or instructions for implementing a standard.
individually identifiable health information (IIHI) [Sec. Rule, §160.103]	Information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a 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.
information security [44 U.S.C., Sec. 3542]	Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide— (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information 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.
information system [Sec. Rule, §164.304]	An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.[142]

[142] [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."

integrity [Sec. Rule, §164.304]	The property that data or information have not been altered or destroyed in an unauthorized manner.
physical safeguards [Sec. Rule, §164.304]	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.
protected health information (PHI) [Sec. Rule, §160.103]	Individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information: (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.
required [Sec. Rule, §164.306(d)(2)]	As applied to an implementation specification (see implementation specification, above), indicating an implementation specification that a covered entity must implement. All implementation specifications are either required or addressable (see "addressable" above).
standard [Sec. Rule, §160.103]	A rule, condition, or requirement: (1) Describing the following information for products, systems, services or practices: (i) Classification of components. (ii) Specification of materials, performance, or operations; or

	(iii) Delineation of procedures; or (2) With respect to the privacy of protected health information.
technical safeguards [Sec. Rule, §164.304]	The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.
user [Sec. Rule, §164.304]	A person or entity with authorized access.

1419

Appendix C—Risk Assessment Tables

Section 3 of this publication provides foundational information about risk assessment as well as an approach that regulated entities may choose to use in assessing risk to ePHI. As part of a risk assessment, regulated entities should identify realistic and probable threats that can have a negative impact on the regulated entity's ability to protect ePHI. Identifying realistic 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 8 - 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

Type of Threat Source	Description	Characteristics

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

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

1429

1430 **Table 9 - Representative Examples – 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).
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.

Threat Events (Characterized by Tactics, Techniques, and Procedures [TTPs])	Description
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, etc.) 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.

Threat Events (Characterized by Tactics, Techniques, and Procedures [TTPs])	Description
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.
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.

Threat Events (Characterized by Tactics, Techniques, and Procedures [TTPs])	Description
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.
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).

Threat Events (Characterized by Tactics, Techniques, and Procedures [TTPs])	Description
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.
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).

Threat Events (Characterized by Tactics, Techniques, and Procedures [TTPs])	Description
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.

Threat Events (Characterized by Tactics, Techniques, and Procedures [TTPs])	Description
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.

1431

1432 **Table 10 - Representative Examples – 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.

Threat Event	Description
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.

1433

1434

Appendix D—National Online Informative References (OLIR) Program

In a general sense, an informative reference, sometimes called a mapping, indicates how one document relates to another document. In the [NIST CSF], for example, six informative references were included (as shown in Figure 1) although many other informative references could have been useful to stakeholders. While the concept of informative references was well received, the static nature of the Cybersecurity Framework and other NIST documents that include informative references meant that some of its informative references became outdated as the documents they referenced were updated.

Subcategory	Informative References
ID.AM-1: Physical devices and systems within the organization are inventoried	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
ID.AM-2: Software platforms and applications within the organization are inventoried	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 · **NIST SP 800-53 Rev. 4** CM-8, PM-5

Figure 1 - Informative References Included in Cybersecurity Framework

Within the context of the National Online Informative References [NIST OLIR] Program, an informative reference indicates the relationship(s) 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. Note that a Focal Document or a Reference Document is not necessarily in a traditional document format (e.g., a formal publication in PDF format) but could be a product, service, or training. A Focal Document Element or a Reference Document Element is a discrete section, sentence, phrase, or other identifiable piece of content of a document.

The OLIR Program is a NIST effort to facilitate subject matter experts (SMEs) in defining standardized relationships between elements of their cybersecurity, privacy, and workforce documents (Reference Documents) and elements of other cybersecurity, privacy, and workforce documents (Focal Documents), like the Cybersecurity Framework Version 1.1 and NIST [SP 800-53], Rev. 5. By removing the informative references from within the 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 National OLIR Program provides an online catalog for displaying, sharing, and comparing informative references. The National OLIR Program offers several benefits, including:

- Provides a single, easy-to-use repository where people can obtain information on many Reference Documents and analyze their relationships
- Increases the transparency, alignment, and harmonization of definitions and concepts across Reference Documents
- Standardizes how References are expressed – making them more consistent, clear, usable, repeatable, and organizable – and provides a way for automation technologies to ingest and utilize them
- Provides the ability to authenticate the source of each Reference and allows users to identify whether the Reference was provided by a verified SME
- Employs mathematical rigor (e.g., standard set theory principles, such as subset, superset, equal, intersect, and discrete logic) to express References rather than merely relying on prose, which can be ambiguous and subjective
- Allows for the cybersecurity and privacy community to keep information current on relationship assertions between Reference Documents and Focal Documents

Before the National OLIR Program, a person analyzing documents was often forced to conduct a manual comparison, typically by copying the contents of both documents into a spreadsheet for easier searching and sorting. To save time, an analyst might try to leverage existing document mappings from SMEs. This laborious and error-prone process would be repeated for all of the elements within the Focal Document and the Reference Document. Multiply this process by numerous analysts performing the task, and two problems quickly emerge: 1) the different opinions of analysts result in inconsistent associations, and 2) the analysts duplicate an enormous amount of effort. Streamlining this process is the main reason the OLIR Derived Relationship Mappings (DRM) capability was created.

DRMs are 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 elements of the Cybersecurity Framework to elements in NIST SP 800-53, Rev. 5. Another informative reference maps elements of the Cybersecurity Framework to elements in two versions of the HITRUST CSF [HITRUST]. A DRM can be created that depicts the relationships between the two Reference Documents: NIST SP 800-53, Rev.5 and 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.

In the context of HIPAA compliance, Table 12 in Appendix E lists mappings between elements of the Security Rule (i.e., standards and implementation specifications); elements of SP 800-53, Rev. 5 (i.e., security and privacy controls); and elements of the Cybersecurity Framework (i.e.,

Subcategory outcomes). Using the included mappings, OLIR catalog, and 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 E—Security Rule Standards and Implementation Specifications Crosswalk

This appendix provides a listing 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 those Security Rule standards and implementation specifications to applicable security controls detailed in NIST [SP 800-53], to the Cybersecurity Framework [NIST CSF] Subcategories, and to NIST publications that are relevant to each Security Rule standard. Readers may draw upon these NIST publications and mappings for consideration in implementing the Security Rule.

The catalog is organized according to the categorization of standards within each of the safeguards sections in the Security Rule. Table 11 provides an overview of the catalog content.

Table 11 - Catalog Headers and Descriptions

Column Headers	Description
Section of HIPAA Security Rule and Standards	Indicates the regulatory citation to the appropriate section of the Security Rule where the standard and implementation specification can be found. Lists the Security Rule Standards.
Implementation Specifications	Lists the implementation specifications associated with the standard, if any exist, and designates the specification as required or addressable (*R = Required, A = Addressable*).
NIST SP 800-53, Rev. 5, Security Controls Mapping	Provides a listing of NIST SP 800-53 security controls that align with the standard and/or implementation specification. These controls may provide value when implementing the particular standards and implementation specifications. For full security control specifications, refer to NIST SP 800-53, Rev.5.
Cybersecurity Framework Subcategory Mapping	Provides a listing of Cybersecurity Framework Subcategories that align with the standard and/or implementation specification. The outcomes of these Subcategories may provide value when implementing the particular standards and implementation specifications.
NIST Publications Crosswalk	Provides a listing of NIST publications that support each particular standard and implementation specification. Publications are listed by publication number. For the full publication title, refer to the *References* within this document.

1523 **Table 12 - Crosswalk of Security Rule to NIST Guidance Documents**

Section of HIPAA Security Rule and Standards	Implementation Specifications	NIST SP 800-53, Rev. 5, Security Controls Mapping	Cybersecurity Framework Subcategory Mapping	NIST Publications Crosswalk
Administrative Safeguards				
164.308(a)(1)(i) **Security Management Process**: Implement policies and procedures to prevent, detect, contain, and correct security violations.		RA-1	ID.GV-1 ID.GV-2 ID.GV-3 ID.GV-4 ID.RA-4 ID.SC-1 ID.SC-2 PR.IP-2 PR.IP-12 DE.CM-8 DE.DP-2 RS.AN-1 RS.AN-5	[FIPS 199] [SP 800-18] [SP 800-30] [SP 800-37] [SP 800-39] [SP 800-53] [SP 800-55] [SP 800-60] [SP 800-84] [SP 800-92] [SP 800-100]
164.308(a)(1)(ii)(A)	**Risk Analysis** (R): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.	RA-2 RA-3	ID.AM-1 ID.AM-2 ID.AM-3 ID.BE-1 ID.BE-2 ID.GV-3 ID.GV-4 ID.RA-1 ID.RA-3 ID.RA-4 ID.RA-5 ID.SC-1 ID.SC-2 PR.DS-3 PR.DS-4 PR.IP-12 RS.AN-5 RS.MI-3	
164.308(a)(1)(ii)(B)	**Risk Management** (R): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).	RA-2 RA-3 PL-2	ID.BE-5 ID.GV-3 ID.GV-4 ID.RA-4 ID.RA-5 ID.RA-6 ID.RM-1 ID.RM-2 ID.RM-3 ID.SC-1 PR.AC-2 PR.DS-4 PR.IP-12 RS.AN-5 RS.MI-3	

Section of HIPAA Security Rule and Standards	Implementation Specifications	NIST SP 800-53, Rev. 5, Security Controls Mapping	Cybersecurity Framework Subcategory Mapping	NIST Publications Crosswalk
164.308(a)(1)(ii)(C)	**Sanction Policy** (R): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	PS-8	ID.GV-3 ID.GV-4 PR.IP-11	
164.308(a)(1)(ii)(D)	**Information System Activity Review** (R): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	AU-6 AU-7 CA-7 IR-5 IR-6 SI-4	ID.GV-3 ID.GV-4 ID.RA-3 ID.RA-5 ID.SC-4 PR.DS-1 PR.DS-5 PR.DS-6 PR.MA-2 PR.PT-1 PR.PT-4 DE.AE-1 DE.AE-3 DE.CM-1 DE.CM-3 DE.CM-4 DE.CM-5 DE.CM-6 DE.CM-7 RS.AN-1	
164.308(a)(2) **Assigned Security Responsibility**: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.		CA-6 PM-2	ID.AM-6 ID.GV-2 ID.GV-3 ID.SC-1 PR.AT-2 PR.AT-4 PR.AT-5 DE.DP-1 RS.CO-1	[SP 800-12] [SP 800-37] [SP 800-53] [SP 800-53A] [SP 800-100]

Section of HIPAA Security Rule and Standards	Implementation Specifications	NIST SP 800-53, Rev. 5, Security Controls Mapping	Cybersecurity Framework Subcategory Mapping	NIST Publications Crosswalk
164.308(a)(3)(i) **Workforce Security**: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.		AC-1 AC-2 AC-3 AC-5 AC-6	ID.AM-6 ID.GV-2 ID.GV-3 ID.RA-3 PR.AC-4 PR.AT-2 PR.AT-4 PR.AT-5 PR.DS-5 PR.IP-11 PR.PT-2 PR.PT-3	[SP 800-12] [SP 800-53]
164.308(a)(3)(ii)(A)	**Authorization and/or Supervision** (A): Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	AC-1 AC-2 AC-3 AC-4 MA-5 MP-2 PS-1 PS-6 PS-7	ID.AM-3 ID.AM-6 ID.GV-2 ID.GV-3 ID.RA-3 PR.AC-4 PR.DS-5 PR.IP-11 PR.MA-1 PR.MA-2 PR.PT-2 PR.PT-3 DE.CM-3 DE.DP-1	
164.308(a)(3)(ii)(B)	**Workforce Clearance Procedure** (A): Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	AC-2 PS-1 PS-2 PS-3 PS-5 PS-6 PS-7	ID.AM-6 ID.GV-2 ID.GV-3 ID.RA-3 PR.AC-1 PR.AC-4 PR.DS-5 PR.IP-11 PR.PT-3 DE.DP-1	
164.308(a)(3)(ii)(C)	**Termination Procedure** (A): Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	PS-1 PS-4 PS-5	ID.AM-6 ID.GV-2 ID.GV-3 ID.RA-3 PR.AC-1 PR.AC-4 PR.DS-5 PR.IP-11 PR.PT-3	

Section of HIPAA Security Rule and Standards	Implementation Specifications	NIST SP 800-53, Rev. 5, Security Controls Mapping	Cybersecurity Framework Subcategory Mapping	NIST Publications Crosswalk
164.308(a)(4)(i) **Information Access Management**: Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.		AC-1 AC-2 AC-5 AC-6	ID.AM-6 ID.GV-2 ID.GV-3 ID.RA-3 PR.AC-1 PR.AC-3 PR.AC-4 PR.AC-6 PR.AC-7 PR.DS-5 PR.DS-7 PR.PT-3 DE.DP-1	[SP 800-12] [SP 800-18] [SP 800-53] [SP 800-63-3] [SP 800-100]
164.308(a)(4)(ii)(A)	**Isolating Healthcare Clearinghouse Functions** (R): If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	AC-5 AC-6 CA-3	ID.AM-4 ID.AM-6 ID.BE-1 ID.BE-2 ID.GV-2 ID.GV-3 ID.RA-3 PR.AC-4 PR.DS-5 PR.DS-7 PR.PT-3 DE.DP-1	
164.308(a)(4)(ii)(B)	**Access Authorization** (A): Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	AC-1 AC-2 AC-3 AC-4 PS-6 PS-7	ID.AM-6 ID.BE-1 ID.BE-2 ID.GV-2 ID.GV-3 ID.RA-3 PR.AC-1 PR.AC-4 PR.AC-5 PR.AC-6 PR.AC-7 PR.DS-5 PR.DS-7 PR.PT-3 DE.DP-1	

Section of HIPAA Security Rule and Standards	Implementation Specifications	NIST SP 800-53, Rev. 5, Security Controls Mapping	Cybersecurity Framework Subcategory Mapping	NIST Publications Crosswalk
164.308(a)(4)(ii)(C)	**Access Establishment and Modification** (A): Implement policies and procedures that, based upon the covered entity's 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.	AC-1 AC-2	ID.AM-6 ID.BE-1 ID.BE-2 ID.GV-2 ID.GV-3 ID.RA-3 PR.AC-1 PR.AC-4 PR.AC-6 PR.AC-7 PR.DS-5 PR.DS-7 PR.PT-3 DE.DP-1	
164.308(a)(5)(i) **Security Awareness and Training**: Implement a security awareness and training program for all members of its workforce (including management).		AT-1 AT-2 AT-3 AT-4	ID.GV-3 PR.AT-1 PR.AT-2 PR.AT-4 PR.AT-5	[SP 800-12] [SP 800-16] [SP 800-50] [SP 800-61] [SP 800-83]
164.308(a)(5)(ii)(A)	**Security Reminders** (A): Periodic security updates.	AT-2 AT-3	ID.GV-3 ID.RA-3 PR.AT-1 PR.AT-2 PR.AT-4 PR.AT-5	
164.308(a)(5)(ii)(B)	**Protection from Malicious Software** (A): Procedures for guarding against, detecting, and reporting malicious software.	AT-2 AT-3	ID.GV-3 PR.AT-1 PR.AT-2 PR.AT-4 PR.AT-5 DE.AE-3 DE.CM-1 DE.CM-4 DE.CM-5 DE.CM-7 RS.CO-2 RS.CO-3 RS.AN-1	

Section of HIPAA Security Rule and Standards	Implementation Specifications	NIST SP 800-53, Rev. 5, Security Controls Mapping	Cybersecurity Framework Subcategory Mapping	NIST Publications Crosswalk
164.308(a)(5)(ii)(C)	**Log-in Monitoring** (A): Procedures for monitoring log-in attempts and reporting discrepancies.	AU-6 AT-3	ID.GV-3 PR.AT-1 PR.AT-2 PR.AT-4 PR.AT-5 PR.PT-1 DE.AE-3 DE.CM-1 DE.CM-3 DE.CM-7 RS.CO-2 RS.CO-3 RS.AN-1	
164.308(a)(5)(ii)(D)	**Password Management** (A): Procedures for creating, changing, and safeguarding passwords.	AT-2 AT-3	ID.GV-3 PR.AC-7 PR.AT-1 PR.AT-2 PR.AT-4 PR.AT-5	
164.308(a)(6)(i) **Security Incident Procedures**: Implement policies and procedures to address security incidents.		IR-1 IR-2 IR-3 IR-4	ID.GV-3 ID.RA-4 PR.IP-9 DE.AE-2 DE.AE-5 RS.CO-1 RS.CO-4 RS.CO-5 RS.AN-3 RC.CO-1 RC.CO-2	[SP 800-12] [SP 800-61] [SP 800-83] [SP 800-86] [SP 800-94]

Section of HIPAA Security Rule and Standards	Implementation Specifications	NIST SP 800-53, Rev. 5, Security Controls Mapping	Cybersecurity Framework Subcategory Mapping	NIST Publications Crosswalk
164.308(a)(6)(ii)	**Response and Reporting** (R): Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	IR-4 IR-5 IR-6 IR-7 IR-8 IR-9	ID.BE-5 ID.GV-3 ID.RA-4 ID.RM-3 PR.IP-8 PR.IP-9 DE.AE-3 DE.AE-4 DE.DP-4 RS.RP-1 RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5 RS.AN-1 RS.AN-2 RS.AN-3 RS.AN-4 RS.AN-5 RS.MI-1 RS.MI-2 RS.MI-3 RC.CO-3	
164.308(a)(7)(i) **Contingency Plan**: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.		CP-1 CP-2	ID.BE-4 ID.BE-5 ID.GV-3 ID.RM-3 ID.SC-5 PR.AC-2 PR.DS-4 PR.IP-1 PR.IP-5 PR.IP-9 PR.PT-5 RS.RP-1 RS.CO-4 RC.RP-1	[FIPS 199] [SP 800-12] [SP 800-18] [SP 800-30] [SP 800-34] [SP 800-60] [SP 800-84]
164.308(a)(7)(ii)(A)	**Data Backup Plan** (R): Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	CP-6 CP-9 CP-9(1)	ID.BE-5 ID.GV-3 PR.AC-2 PR.DS-4 PR.IP-1 PR.IP-4 PR.IP-9 PR.PT-5 RS.RP-1 RS.CO-1 RS.CO-4 RC.RP-1	

Section of HIPAA Security Rule and Standards	Implementation Specifications	NIST SP 800-53, Rev. 5, Security Controls Mapping	Cybersecurity Framework Subcategory Mapping	NIST Publications Crosswalk
164.308(a)(7)(ii)(B)	**Disaster Recovery Plan** (R): Establish (and implement as needed) procedures to restore any loss of data.	CP-2 CP-6 CP-7 CP-8 CP-9 CP-10	ID.BE-3 ID.BE-5 ID.GV-3 ID.SC-5 PR.DS-4 PR.IP-1 PR.IP-4 PR.IP-9 PR.PT-5 RS.RP-1 RS.CO-1 RS.CO-4 RS.AN-2 RC.RP-1 RC.CO-3	
164.308(a)(7)(ii)(C)	**Emergency Mode Operation Plan** (R): Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	CP-2 CP-10	ID.BE-1 ID.BE-2 ID.BE-3 ID.BE-5 ID.GV-3 ID.RM-3 PR.DS-4 PR.IP-1 PR.IP-5 PR.IP-9 PR.PT-5 RS.RP-1 RS.CO-1 RS.CO-4 RS.AN-2 RC.RP-1 RC.CO-3	
164.308(a)(7)(ii)(D)	**Testing and Revision Procedure** (A): Implement procedures for periodic testing and revision of contingency plans.	CP-2 CP-3 CP-4	ID.BE-3 ID.BE-5 ID.GV-3 ID.RA-5 ID.SC-5 PR.DS-4 PR.IP-1 PR.IP-4 PR.IP-7 PR.IP-9 PR.IP-10 PR.PT-5 RS.CO-4 RS.IM-1 RS.IM-2 RC.RP-1 RC.IM-1 RC.IM-2	

Section of HIPAA Security Rule and Standards	Implementation Specifications	NIST SP 800-53, Rev. 5, Security Controls Mapping	Cybersecurity Framework Subcategory Mapping	NIST Publications Crosswalk
164.308(a)(7)(ii)(E)	**Applications and Data Criticality Analysis** (A): Assess the relative criticality of specific applications and data in support of other contingency plan components.	CP-2 CP-2(8) RA-2 RA-2(1)	ID.AM-2 ID.AM-5 ID.BE-1 ID.BE-2 ID.BE-3 ID.BE-4 ID.BE-5 ID.GV-3 ID.RA-1 ID.RA-4 ID.RA-5 ID.RM-3 ID.SC-2 PR.DS-4 PR.IP-1 PR.IP-9 PR.PT-5 RS.CO-4 RS.AN-2 RC.RP-1	
164.308(a)(8) **Evaluation**: Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.		CA-1 CA-2 CA-6 CA-7 CA-8	ID.AM-3 ID.BE-1 ID.BE-2 ID.BE-5 ID.GV-3 ID.RA-1 ID.RA-4 ID.SC-1 ID.SC-4 PR.IP-1 PR.IP-3 PR.IP-7 DE.AE-3 DE.CM-1 DE.CM-8 DE.DP-2 DE.DP-5 RS.IM-1 RS.IM-2 RC.IM-1 RC.IM-2	[SP 800-12] [SP 800-37] [SP 800-53A] [SP 800-55] [SP 800-84] [SP 800-115]

Section of HIPAA Security Rule and Standards	Implementation Specifications	NIST SP 800-53, Rev. 5, Security Controls Mapping	Cybersecurity Framework Subcategory Mapping	NIST Publications Crosswalk
164.308(b)(1) **Business Associate Contracts and Other Arrangements**: 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 Sec. 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.		CA-3 PS-7 SA-9	ID.AM-4 ID.AM-6 ID.GV-2 ID.GV-3 ID.GV-4 ID.SC-3 PR.AC-3 PR.AT-3 PR.DS-1 PR.DS-2	[SP 800-12] [SP 800-37] [SP 800-47] [SP 800-100]
164.308(b)(3)	**Written Contract or Other Arrangement** (R): Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).	CA-3 SA-4 SA-9	ID.AM-4 ID.GV-2 ID.GV-3 ID.GV-4 ID.SC-3 ID.SC-4 PR.AT-3	
Physical Safeguards				
164.310(a)(1) **Facility Access Controls**: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.		PE-1 PE-2 PE-3 PE-3(1) PE-4 PE-5	ID.GV-3 ID.RA-1 ID.RA-3 PR.AC-2 PR.AC-5 PR.IP-5 DE.CM-7	[SP 800-12] [SP 800-18] [SP 800-30] [SP 800-34] [SP 800-53]

Section of HIPAA Security Rule and Standards	Implementation Specifications	NIST SP 800-53, Rev. 5, Security Controls Mapping	Cybersecurity Framework Subcategory Mapping	NIST Publications Crosswalk
164.310(a)(2)(i)	**Contingency Operations** (A): Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	CP-2 CP-6 CP-7 PE-2 PE-3 PE-17	ID.BE-1 ID.BE-2 ID.BE-3 ID.BE-4 ID.BE-5 ID.GV-3 ID.RM-3 ID.SC-5 PR.AC-2 PR.DS-4 PR.IP-4 PR.IP-5 PR.IP-9 PR.PT-5 RS.RP-1 RS.CO-1 RS.CO-4 RC.RP-1 RC.CO-3	
164.310(a)(2)(ii)	**Facility Security Plan** (A): Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	PE-1 PL-2	ID.AM-1 ID.GV-3 PR.AC-2 PR.DS-3 PR.IP-5 DE.CM-2 DE.CM-7	
164.310(a)(2)(iii)	**Access Control and Validation Procedures** (A): Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	PE-1 PE-2 PE-3 PE-3(1) PE-6 PE-8	ID.GV-3 ID.RA-3 PR.AC-2 PR.AC-4 PR.DS-3 PR.IP-5 PR.PT-3 DE.CM-2 DE.CM-7 DE.DP-1	

Section of HIPAA Security Rule and Standards	Implementation Specifications	NIST SP 800-53, Rev. 5, Security Controls Mapping	Cybersecurity Framework Subcategory Mapping	NIST Publications Crosswalk
164.310(a)(2)(iv)	**Maintenance Records** (A): Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	MA-1[143] MA-2 MA-6	ID.GV-3 PR.DS-3 PR.IP-5 PR.MA-1 PR.PT-1	
164.310(b) **Workstation Use**: Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.		AC-3 AC-4 AC-11 AC-12 AC-16 AC-17 AC-19 PE-3 PE-5 PL-4 PS-6	ID.GV-3 PR.AC-2 PR.AC-3 PR.AC-4 PR.AC-5 PR.DS-5 PR.IP-5 PR.PT-3 DE.CM-7	[SP 800-12] [SP 800-53]
164.310(c) **Workstation Security**: Implement physical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.		MP-2 MP-3 MP-4 PE-2 PE-3 PE-4 PE-5 PE-18	ID.GV-3 PR.AC-2 PR.DS-5 PR.DS-8 PR.IP-5 PR.PT-3 DE.CM-7	[SP 800-12] [SP 800-53]

[143] In [SP 800-53], the Maintenance security control family discusses maintenance activities related to information systems. The same principles, however, can be applied to facility maintenance.

Section of HIPAA Security Rule and Standards	Implementation Specifications	NIST SP 800-53, Rev. 5, Security Controls Mapping	Cybersecurity Framework Subcategory Mapping	NIST Publications Crosswalk
164.310(d)(1) **Device and Media Controls**: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.		CM-8 MP-1 MP-2 MP-3 MP-4 MP-5 MP-6 PE-16 PE-20	ID.AM-1 ID.AM-3 ID.GV-3 PR.AC-2 PR.DS-1 PR.DS-3 PR.IP-5 PR.MA-2 PR.PT-2 DE.CM-7	[SP 800-12] [SP 800-34] [SP 800-53] [SP 800-88]
164.310(d)(2)(i)	**Disposal** (R): Implement policies and procedures to address the final disposition of electronic protected health information and/or the hardware or electronic media on which it is stored.	MP-6	ID.AM-1 ID.AM-3 ID.GV-3 PR.DS-1 PR.DS-3 PR.IP-5 PR.IP-6 PR.PT-2	
164.310(d)(2)(ii)	**Media Re-use** (R): Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	MP-6	ID.AM-1 ID.AM-3 ID.GV-3 PR.DS-1 PR.DS-3 PR.IP-5 PR.IP-6 PR.MA-2 PR.PT-2	
164.310(d)(2)(iii)	**Accountability** (A): Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	CM-8 MP-5 PE-16 PE-20 PS-6	ID.AM-1 ID.AM-3 ID.GV-3 PR.AC-2 PR.DS-1 PR.DS-3 PR.DS-8 PR.IP-5 PR.MA-2 PR.PT-1 PR.PT-2 DE.AE-3 DE.CM-7	

Section of HIPAA Security Rule and Standards	Implementation Specifications	NIST SP 800-53, Rev. 5, Security Controls Mapping	Cybersecurity Framework Subcategory Mapping	NIST Publications Crosswalk
164.310(d)(2)(iv)	**Data Backup and Storage** (A): Create a retrievable exact copy of electronic protected health information, when needed, before movement of equipment.	CP-9 MP-4	ID.AM-1 ID.AM-3 ID.GV-3 PR.DS-1 PR.DS-3 PR.DS-4 PR.IP-4 PR.IP-5 PR.PT-2 PR.PT-5	
Technical Safeguards				
164.312(a)(1) **Access Control**: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).		AC-1 AC-3 AC-5 AC-6	ID.GV-3 ID.RA-1 ID.RA-3 PR.AC-4 PR.AC-5 PR.AC-6 PR.AC-7 PR.DS-1 PR.DS-5 PR.MA-2 PR.PT-2 PR.PT-3 PR.PT-4 DE.DP-1	[SP 800-12] [SP 800-34] [SP 800-53] [SP 800-63-3] [FIPS 140-3]
164.312(a)(2)(i)	**Unique User Identification** (R): Assign a unique name and/or number for identifying and tracking user identity.	AC-2 AC-3 IA-2 IA-3 IA-4 IA-8	ID.GV-3 PR.AC-1 PR.AC-4 PR.AC-6 PR.DS-5 PR.MA-2 PR.PT-3 DE.CM-3	
164.312(a)(2)(ii)	**Emergency Access Procedure** (R): Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	AC-2 AC-3 CP-2	ID.BE-4 ID.BE-5 ID.GV-3 PR.AC-1 PR.AC-4 PR.AC-7 PR.DS-4 PR.DS-5 PR.IP-9 PR.MA-2 PR.PT-3 PR.PT-5 DE.DP-1 RS.RP-1 RS.CO-1 RS.CO-4	

Section of HIPAA Security Rule and Standards	Implementation Specifications	NIST SP 800-53, Rev. 5, Security Controls Mapping	Cybersecurity Framework Subcategory Mapping	NIST Publications Crosswalk
164.312(a)(2)(iii)	**Automatic Logoff** (A): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	AC-12	ID.GV-3 PR.AC-1 PR.DS-1 PR.DS-5 PR.MA-2	
164.312(a)(2)(iv)	**Encryption and Decryption** (A): Implement a mechanism to encrypt and decrypt electronic protected health information.	SC-13	ID.GV-3 PR.DS-1 PR.DS-5 PR.MA-2 PR.PT-2 PR.PT-3	
164.312(b) **Audit Controls**: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.		AU-1 AU-2 AU-3 AU-4 AU-6 AU-7 AU-8	ID.GV-3 PR.AC-5 PR.AC-6 PR.DS-1 PR.DS-6 PR.MA-2 PR.PT-1 PR.PT-2 PR.PT-4 DE.AE-1 DE.AE-3 DE.CM-1 DE.CM-3 DE.CM-7 RS.AN-1	[SP 800-12] [SP 800-53] [SP 800-53A] [SP 800-55] [SP 800-92] [SP 800-115]
164.312(c)(1) **Integrity**: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.		CP-9 MP-2 MP-5 SC-8 SI-1 SI-7	ID.GV-3 ID.RA-3 PR.AC-5 PR.DS-1 PR.DS-6 PR.DS-8	[SP 800-12] [SP 800-53] [SP 800-106] [SP 800-107]
164.312(c)(2)	**Mechanism to Authenticate Electronic Protected Health Information** (A): Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	SC-8 SI-7	ID.GV-3 ID.RA-3 PR.AC-5 PR.DS-1 PR.DS-6	
164.312(d) **Person or Entity Authentication**: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.		IA-2 IA-3 IA-4 IA-8 IA-9	ID.GV-3 PR.AC-1 PR.AC-6 PR.AC-7 PR.DS-1 PR.MA-2 DE.CM-3	[FIPS 200] [SP 800-12] [SP 800-53] [SP 800-63-3]

Section of HIPAA Security Rule and Standards	Implementation Specifications	NIST SP 800-53, Rev. 5, Security Controls Mapping	Cybersecurity Framework Subcategory Mapping	NIST Publications Crosswalk
164.312(e)(1) **Transmission Security**: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.		SC-8	ID.GV-3 ID.RA-3 PR.AC-3 PR.AC-5 PR.DS-2 PR.DS-5 PR.MA-2 PR.PT-4 DE.CM-3	[FIPS 140-3] [SP 800-12] [SP 800-41] [SP 800-45] [SP 800-46] [SP 800-52] [SP 800-53] [SP 800-58] [SP 800-63-3] [SP 800-77] [SP 800-81] [SP 800-113]
164.312(e)(2)(i)	**Integrity Controls** (A): Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	SC-8 SI-7	ID.GV-3 ID.RA-3 PR.AC-5 PR.DS-2 PR.DS-5 PR.DS-6 PR.MA-2 PR.PT-4 DE.CM-1 DE.CM-3	
164.312(e)(2)(ii)	**Encryption** (A): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	SC-8 SC-12 SC-13	ID.GV-3 ID.RA-3 PR.AC-3 PR.AC-5 PR.DS-2 PR.DS-5 PR.MA-2 PR.PT-4 DE.CM-3	
Organizational Requirements				
164.314(a)(1) **Business Associate Contracts or Other Arrangements**: The contract or other arrangement between the covered entity and its business associate required by § 164.308(b) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.		PS-6 PS-7 SA-4 SA-9	ID.AM-4 ID.AM-6 ID.BE-1 ID.BE-2 ID.BE-4 ID.GV-2 ID.GV-3 ID.RA-3 ID.SC-2 ID.SC-3 ID.SC-4 PR.AT-3	[SP 800-35] [SP 800-39] [SP 800-47] [SP 800-100]

Section of HIPAA Security Rule and Standards	Implementation Specifications	NIST SP 800-53, Rev. 5, Security Controls Mapping	Cybersecurity Framework Subcategory Mapping	NIST Publications Crosswalk
164.314(a)(2)(i)	**Business Associate Contracts** (R): The contract must provide that the business associate will-- (A) Comply with the applicable requirements of this subpart; (B) In accordance with 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information 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; and (C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.	IR-6 PS-6 PS-7 SA-4 SA-9	ID.AM-4 ID.AM-6 ID.BE-1 ID.BE-2 ID.GV-2 ID.GV-3 ID.RA-3 ID.RA-6 ID.SC-2 ID.SC-3 ID.SC-4 PR.AT-3 DE.AE-3 DE.DP-4 RS.CO-2 RS.CO-3 RC.CO-3	
164.314(a)(2)(ii)	**Other Arrangements** (R): The 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).	CA-3 PS-6 PS-7 SA-9	ID.AM-4 ID.AM-6 ID.BE-1 ID.BE-2 ID.GV-2 ID.GV-3 ID.RA-3 ID.SC-2 ID.SC-3 ID.SC-4 PR.AT-3	
164.314(a)(2)(iii)	**Business associate contracts with subcontractors** (R): 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.	IR-6 PS-6 PS-7 SA-4 SA-9	ID.AM-4 ID.AM-6 ID.BE-1 ID.BE-2 ID.GV-2 ID.GV-3 ID.RA-3 ID.RA-6 ID.SC-2 ID.SC-3 ID.SC-4 PR.AT-3 DE.AE-3 DE.DP-4 RS.CO-2 RS.CO-3 RC.CO-3	

Section of HIPAA Security Rule and Standards	Implementation Specifications	NIST SP 800-53, Rev. 5, Security Controls Mapping	Cybersecurity Framework Subcategory Mapping	NIST Publications Crosswalk
164.314(b)(1) **Requirements for Group Health Plans**: Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.		PL-2	ID.AM-6 ID.BE-1 ID.BE-2 ID.GV-2 ID.GV-3 ID.RA-3 ID.SC-2 ID.SC-3 ID.SC-4	[SP 800-35] [SP 800-39] [SP 800-47] [SP 800-61] [SP 800-100]
164.314(b)(2)(i)	**Group Health Plan Implementation Specification** (R): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan.	PL-2	ID.AM-6 ID.BE-1 ID.BE-2 ID.BE-4 ID.BE-5 ID.GV-2 ID.GV-3 ID.RA-3 ID.SC-2 ID.SC-3 ID.SC-4 PR.DS-1 PR.DS-2 DE.CM-7	
164.314(b)(2)(ii)	**Group Health Plan Implementation Specification** (R): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (ii) Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures.	PL-2	ID.AM-6 ID.BE-1 ID.BE-2 ID.GV-2 ID.GV-3 ID.RA-3 ID.SC-2 ID.SC-3 ID.SC-4	

Section of HIPAA Security Rule and Standards	Implementation Specifications	NIST SP 800-53, Rev. 5, Security Controls Mapping	Cybersecurity Framework Subcategory Mapping	NIST Publications Crosswalk
164.314(b)(2)(iii)	**Group Health Plan Implementation Specification** (R): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information.	SA-9	ID.AM-6 ID.BE-1 ID.BE-2 ID.GV-2 ID.GV-3 ID.RA-3 ID.SC-2 ID.SC-3 ID.SC-4	
164.314(b)(2)(iv)	**Group Health Plan Implementation Specification** (R): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-- (iv) Report to the group health plan any security incident of which it becomes aware.	IR-6	ID.AM-6 ID.BE-1 ID.BE-2 ID.GV-2 ID.GV-3 ID.RA-3 ID.RA-6 ID.SC-3 ID.SC-4	
Policies and Procedures and Documentation Requirements				
164.316(a) **Policies and Procedures**: Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity 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.		PL-1 PL-2 RA-1 RA-3	ID.BE-1 ID.BE-2 ID.BE-3 ID.GV-1 ID.GV-3 ID.RA-3 ID.RA-4 ID.RA-5 ID.SC-1	[SP 800-12] [SP 800-100]

Section of HIPAA Security Rule and Standards	Implementation Specifications	NIST SP 800-53, Rev. 5, Security Controls Mapping	Cybersecurity Framework Subcategory Mapping	NIST Publications Crosswalk
164.316(b)(1) **Documentation**: (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.		CA-2 PL-2	ID.BE-1 ID.BE-2 ID.BE-3 ID.GV-1 ID.GV-3 ID.RA-3 ID.SC-1	[SP 800-18] [SP 800-53] [SP 800-53A]
164.316(b)(2)(i)	**Time Limit** (R): Retain the documentation required by paragraph (b)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.	SI-12	ID.AM-4 ID.BE-1 ID.BE-2 ID.BE-3 ID.GV-1 ID.GV-3 ID.RA-3 ID.SC-1	
164.316(b)(2)(ii)	**Availability** (R): Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	All of the -1 controls for each of the control families	ID.AM-4 ID.BE-1 ID.BE-2 ID.BE-3 ID.GV-1 ID.GV-3 ID.RA-3 ID.SC-1	
164.316(b)(2)(iii)	**Updates** (R): Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	All of the -1 controls for each of the control families PL-2	ID.AM-4 ID.BE-1 ID.BE-2 ID.BE-3 ID.GV-1 ID.GV-3 ID.RA-1 ID.RA-3 ID.SC-1 PR.IP-5 PR.IP-7 RS.IM-1 RC.IM-1	

1524

Appendix F—HIPAA Security Rule Resources (Informative)

This appendix lists resources (e.g., guidance, templates, tools) that regulated entities may find useful for complying with the Security Rule [Sec. Rule] and improving the security posture of their organizations. 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. It is expected that regulated entities could consult these resources when they need additional information or guidance about a particular topic.

Risk Assessment/Risk Management: The assessment, analysis, and management of risk to ePHI provides the foundation for a regulated entity's Security Rule compliance efforts. While regulated entities are free to use any risk assessment/management methodology that effectively protects the confidentiality, integrity, and availability of ePHI, the resources listed may be helpful.

- **Security Risk Assessment Tool** [SRA Tool] – Designed to help regulated entities conduct a security risk assessment as required by the HIPAA Security Rule. Regulated entities should 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's risk analysis requirement.
- **Security Risk Assessment Tool v3.2 User Guide** – Assists regulated entities in completing the SRA tool.
- **Framework for Improving Critical Infrastructure Cybersecurity** [NIST CSF] – Consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps the owners and operators of critical infrastructure manage cybersecurity-related risk.
- **Health Industry Cybersecurity Practices (HICP) Managing Threats and Protecting Patients** – Sets forth a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cybersecurity risks for regulated entities.
- **Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations** – Contains technical details for implementing cybersecurity practices. It provides an overview of cybersecurity practices that have been outlined by the industry as highly effective at mitigating risks to the healthcare industry.
- **Protecting the Healthcare Digital Infrastructure: Cybersecurity Checklist** – Outlines several hardware, software, and cybersecurity educational items that organizations should consider and implement to protect their digital infrastructure.
- **Health Sector Cybersecurity Coordination Center (HC3) Threat Briefs** – Highlights relevant cybersecurity topics and raises the Healthcare and Public Health (HPH) sector's situational awareness of current cyber threats, threat actors, best practices, and mitigation tactics.
- **Health Sector Cybersecurity Coordination Center (HC3) Sector Alerts** – Provides high-level, situational background information and context for technical and executive audiences. Designed to assist the sector with the defense of large-scale and high-level vulnerabilities.

- **Healthcare Sector Cybersecurity Framework Implementation Guide** – Helps HPH Sector organizations understand and use the HITRUST Risk Management Framework – which consists of the [HITRUST] CSF, CSF Assurance Program, and supporting methodologies – to implement the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) in the HPH Sector and meet its objectives for critical infrastructure protection.
- **HICP Managing Threats and Protecting Patients: Resources and Templates** – Maps the 10 most effective practices to mitigate common threats in the healthcare sector to Subcategories of the Cybersecurity Framework. An evaluation methodology is also provided to assist regulated entities with selecting and prioritizing the practices of greatest relevance.
- **HICP Quick-Start Guide for Medium/Large Practices** – Provides practical, cost-effective practices that help strengthen an organization against cyber criminals, seamlessly integrate cybersecurity into day-to-day operations, and outline an effective strategy to reduce enterprise cybersecurity risk.
- **HICP Threat Mitigation Matrix** – Assists an organization's IT team in identifying the five key cybersecurity threats outlined in the HICP that are most pertinent to their unique organization and apply controls to mitigate those threats. The controls and sub-controls are categorized based on their applicability to the organization's size.
- **Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy** [SP 800-37] – Provides a disciplined, structured, and flexible process for managing security and privacy risk.
- **Managing Information Security Risk: Organization, Mission, and Information System View** [SP 800-39] – Provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation) and organizational assets.
- **Top 10 Myths of Security Risk Analysis** – Includes an informative list of common misconceptions about HIPAA and a risk assessment to help distinguish fact from fiction.
- **OCR Audit Protocol** – Reviews the policies and procedures adopted and employed by covered entities and business associates to meet the selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules.
- **MITRE ATT&CK** – Consists of a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies.
- **Integrating Cybersecurity and Enterprise Risk Management (ERM)** [IR 8286] – Helps enterprises and their component organizations better identify, assess, and manage their cybersecurity risks in the context of their broader mission and business objectives.
- **Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management** [IR 8286A] – Describes documentation of various scenarios based on the potential impact of threats and vulnerabilities on enterprise assets.

Documentation Templates: Regulated entities may find value in utilizing templates that facilitate the creation of required documentation.

- **Sample Business Associate Agreement (BAA) Provisions** – Includes sample business associate agreement provisions to help covered entities and business associates more

easily comply with the business associate contract requirements. While these sample provisions are written for the purposes of the contract between a covered entity and its business associate, the language may be adapted for a contract between a business associate and subcontractor.

- **HICP Managing Threats and Protecting Patients: Resources and Templates** – Provides practical document templates that can be used by regulated entities to aid in strengthening the privacy, security, and cybersecurity protocols of their organizations.

Small Regulated Entities: Smaller regulated entities with limited resources may face additional challenges in complying with the Security Rule's requirements. These resources may provide smaller organizations with the guidance needed to improve their cybersecurity posture while complying with the Security Rule.

- **Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations** – Provides small healthcare organizations with a series of cybersecurity practices to reduce the impact of the five cybersecurity threats identified in *HICP Managing Threats and Protecting Patients*. Small organizations may benefit from the cybersecurity practices in both volumes.
- **Guide to Privacy and Security of Electronic Health Information** – Aims to help small, regulated entities understand how to integrate federal health information privacy and security requirements into their practices.
- **Security Standards: Implementation for the Small Provider** – Provides guidance concerning the implementation of the Security Rule standards, implementation specifications, and requirements as they relate to covered entities that are sole practitioners or otherwise considered small providers.
- **HICP Quick Start Guide for Small Practices** – Gives small healthcare organizations practical, cost-effective practices that lessen cybersecurity risks by improving organizational "cyber hygiene."
- **NIST Small Business Cybersecurity Corner** – Provides cybersecurity resources tailored to protect small businesses and reduce their cybersecurity risks.
- **Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide** [SP 1271] – Details cybersecurity activities for each Function of the Cybersecurity Framework that may be good starting points for small businesses.
- **Cybersecurity for Small Business: Protect Your Small Business** – Focuses on the basics for protecting a small business from cyber attacks. The business cybersecurity resources in this section were developed in partnership with NIST, the U.S. Small Business Administration, and the Department of Homeland Security.
- **Resources for Small and Midsize Businesses** – Describes Cybersecurity and Infrastructure Security Agency (CISA) resources to help small and medium businesses address their cybersecurity risks.
- **Small Business Information Security: The Fundamentals** [NISTIR 7621] – Presents the fundamentals of a small business information security program in non-technical language.

Telehealth/Telemedicine Guidance: Telehealth and telemedicine technologies can provide advantages to delivering patient care. However, new risks to ePHI can also be introduced.

Regulated entities need to consider the security practices of the telehealth platforms that they utilize. Consideration must also be given to where telehealth meetings are taking place. Are personnel present who do not have authorization to access PHI? Are any devices (e.g., IoT devices) present that are listening and/or recording?

- **Health Industry Cybersecurity – Securing Telehealth and Telemedicine (HIC-STAT)** – Identifies cyber risks and best practices associated with the use of telehealth and telemedicine and summarizes the policy and regulatory underpinnings for telehealth and telemedicine cyber risk management. Its target audience includes senior executives in healthcare and IT, telehealth service and product companies, and regulators.
- **Tips for Video Conferencing** – Details useful CISA tips for conducting secure video conferencing that can apply to telehealth and telemedicine.
- **Guidance for Securing Video Conferencing** – Presents cybersecurity principles and practices that individuals and organizations can follow to video conference more securely.

Mobile device security: Physicians, healthcare providers, and other healthcare professionals use smartphones, laptops, and tablets in their work. The U.S. Department of Health and Human Services has gathered these tips and information to help protect and secure health information when using mobile devices.

- **How Can You Protect and Secure Health Information When Using a Mobile Device?** – Provides suggestions for how to secure mobile devices.
- **Managing Mobile Devices in Your Health Care Organization** – Details five steps that an organization can take to help manage mobile devices
- **A Guide to Understanding Your Organization's Mobile Device Policies and Procedures Fact Sheet** – Helps healthcare providers and professionals understand their organization's mobile device policies and procedures.
- **Using a Mobile Device: How to Protect and Secure Health Information Brochure** – Provides healthcare providers and professionals with tips for understanding how to protect and secure patient health information when using a mobile device in a public space, home, office, or healthcare facility.
- **Guidelines for Managing the Security of Mobile Devices in the Enterprise** [SP 800-124] – Explains the security concerns inherent in mobile device use and provides recommendations for selecting, implementing, and using technologies to centrally manage and secure mobile devices against a variety of threats.

Cloud services: Like many technologies, cloud services can provide benefits to patient care and can also assist regulated entities in complying with the Security Rule. However, cloud services can also introduce risks to ePHI. These resources may help regulated entities understand, select, and manage cloud services.

- **Guidance on HIPAA and Cloud Computing** – Assists regulated entities, including cloud service providers (CSPs), in understanding their HIPAA obligations.

- **Cloud Security Basics** – Provides foundational information about cloud services – both their benefits and the risks introduced – so that organizations can make informed decisions before procuring a CSP.
- **Cloud Computing Synopsis and Recommendations** [SP 800-146] – Provides the NIST-established definition for cloud computing, describes cloud computing benefits and open issues, presents an overview of major classes of cloud technology, and provides recommendations on how organizations should consider the relative opportunities and risks of cloud computing.
- **Guidelines on Security and Privacy in Public Cloud Computing** [SP 800-144] – Provides an overview of the security and privacy challenges pertinent to public cloud computing and points out considerations that organizations should take when outsourcing data, applications, and infrastructure to a public cloud environment.
- **General Access Control Guidance for Cloud Systems** [SP 800-210] – Presents cloud access control characteristics and a set of general access control guidance for cloud service models.

Ransomware & Phishing: New threats are constantly emerging. The resources below can help regulated entities protect ePHI from ransomware and phishing, two common threats. The recommendations in these resources may also help regulated entities protect ePHI from a variety of other threats.

- **FACT SHEET: Ransomware and HIPAA** – Describes ransomware attack prevention and recovery from a healthcare sector perspective, including the role that HIPAA plays in assisting regulated entities to prevent and recover from ransomware attacks and how HIPAA breach notification processes should be managed in response to a ransomware attack.
- **Stop Ransomware** – Designed to help individuals and organizations prevent attacks that can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services.
- **HICP Ransomware Attack Fact Sheet** – Provides information and guidance on mitigating ransomware attacks.
- **HICP Ransomware Threat Slides** – Provides information and guidance on mitigating ransomware attacks.
- **Ransomware Guidance** – Illustrates how ransomware attacks can happen and how to stay prepared, get helpful information, and find support.
- **Tips and Tactics: Ransomware** – Gives steps to protect an organization from the threat of ransomware and to help recover from a ransomware attack.
- **Tips and Tactics: Preparing Your Organization for Ransomware Attacks** – Includes basic practices for protecting against and recovering from ransomware attacks.
- **Prepare, React, and Recover from Ransomware** – Provides industry-tested best practices (Prepare, React, Recover) to ensure that an organization is prepared for ransomware attacks and can continue to keep patients safe in the event of an attack.
- **Ransomware Prevention and Response for Chief Information Security Officers (CISO)** – Assembles existing Federal Government and private industry best practices and mitigation strategies focused on the prevention and response to ransomware incidents.

- **HICP Email Phishing Fact Sheet** – Provides information and guidance on recognizing and mitigating phishing attacks.
- **HICP Email Phishing Threat Slides** – Provides information and guidance on recognizing and mitigating phishing attacks.
- **Phishing Guidance** – Provides information about common types of phishing messages and why any business owner or employee needs to be vigilant against their danger. This resource also helps in learning how to stay prepared, get helpful information, and find support.

Education, Training, and Awareness: Cybersecurity risk management and compliance with the Security Rule are ongoing activities that require the support of organizational personnel. The resources below can help regulated entities develop and maintain programs that invest in the education, training, and awareness of personnel.

- **Cybersecurity Newsletters Archive** – Helps HIPAA-covered entities and business associates remain in compliance with the HIPAA Security Rule by identifying emerging or prevalent issues and highlighting best practices to safeguard PHI.
- **405(d) Awareness Products & Resources** – Provides resources to engage with the whole HPH Sector on cybersecurity. The News and Awareness Resources can be printed and downloaded.
- **Mobile Devices: Know the RISKS. Take the STEPS. PROTECT and SECURE Health Information Presentation** – Assists healthcare organizations in creating a culture of awareness among their healthcare providers, professionals, and staff. The available presentation provide training on how to protect and secure patient health information when using a mobile device.
- **Security Risk Assessment Videos** – Includes informative videos about conducting risk assessments and using the SRA Tool.
- **Cybersecurity for Small Business: Protect Your Small Business** – Presents the basics for protecting a business from cyber attacks. The business cybersecurity resources in this section were developed in partnership with NIST, the U.S. Small Business Administration, and the Department of Homeland Security.
- **HHS Office of the Chief Information Officer (OCIO) Security Awareness Training** – Includes a comprehensive list of the HHS OCIO information security and role-based training resources that address topics such as phishing, executive and managerial training, and IT administration.
- **InfraGard** – Details a partnership between the Federal Bureau of Investigation (FBI) and members of the private sector for the protection of U.S. Critical Infrastructure. InfraGard connects owners and operators in critical infrastructure with the FBI to provide education, share information, network, and hold workshops on emerging technologies and threats.
- **Security Rule Educational Paper Series** – Presents a group of educational papers that are designed to give regulated entities insight into the Security Rule and assistance with implementation of the security standards.
    - **Security 101 for Covered Entities** – Provides an overview of the Security Rule and its intersection with the HIPAA Privacy Rule.

- **Administrative Safeguards** – Provides information and considerations for regulated entities for the standards and implementation specifications of the Administrative safeguards in the Security Rule.
- **Physical Safeguards** – Provides information and considerations for regulated entities for the standards and implementation specifications of the Physical safeguards in the Security Rule.
- **Technical Safeguards** – Provides information and considerations for regulated entities for the standards and implementation specifications of the Technical safeguards in the Security Rule.
- **Organizational, Policies and Procedures and Documentation Requirements** – Presents the standards for Organizational Requirements and Policies and Procedures and Documentation Requirements, as well as their implementation specifications.

Medical Device and Medical IoT Security: Connected medical devices are an important component of modern patient care. However, precautions must be taken to securely integrate these devices into organizational networks and to protect ePHI. The resources below can assist regulated entities in these efforts.

- **FDA Medical Device Cybersecurity** – Presents updates, risks, reports, and medical device guidance for product manufacturers and health delivery organizations.
- **Medical Device and Health IT Joint Security Plan** – Provides a total product life cycle reference guide to developing, deploying, and supporting cyber secure technology solutions in the healthcare environment.
- **HICP Fact Sheet – Attacks Against Connected Medical Devices** – Provides information and guidance on mitigating medical device attacks.
- **HICP Threat Slides – Attacks Against Connected Medical Devices** – Provides information and guidance on mitigating medical device attacks.
- **The FDA's Role in Medical Device Cybersecurity** – Discusses myths and facts about medical device cybersecurity in a table geared toward manufacturers and providers.
- **Postmarket Management of Cybersecurity in Medical Devices** – Helps manufacturers and healthcare providers manage cybersecurity in medical devices, particularly those that are networked.
- **Electronic Health Records on Mobile Devices** – Provides a modular, open, end-to-end reference design that can be tailored and implemented by healthcare organizations of varying sizes and information technology (IT) sophistication. The guide shows how healthcare providers can use open-source and commercially available tools and technologies to more securely share patient information with caregivers who are using mobile devices.
- **Securing Wireless Infusion Pumps** – Demonstrates how healthcare delivery organizations (HDOs) can use standards-based, commercially available cybersecurity technologies to better protect the infusion pump ecosystem, including patient information and drug library dosing limits.
- **Securing Picture Archiving and Communication System (PACS)** – Provides an example implementation that demonstrates how HDOs can use standards-based, commercially available cybersecurity technologies to better protect a PACS ecosystem.

- **Foundational Cybersecurity Activities for IoT Device Manufacturers** [IR 8259] – Describes recommended activities related to cybersecurity that manufacturers should consider performing before their IoT devices are sold to customers.
- **IoT Device Cybersecurity Capability Core Baseline** [IR 8259A] – Provides organizations with a starting point to use in identifying the device cybersecurity capabilities for new IoT devices that they will manufacture, integrate, or acquire.
- **IoT Non-Technical Supporting Capability Core Baseline** [IR 8259B] – Provides organizations with a starting point to use in identifying the non-technical supporting capabilities needed in relation to IoT devices that they will manufacture, integrate, or acquire.
- **Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks** [IR 8228] – Aims to help federal agencies and other organizations better understand and manage the cybersecurity and privacy risks associated with their individual IoT devices throughout the devices' life cycles.

Protection of Organizational Resources and Data: Protecting the confidentiality, integrity, and availability of ePHI is paramount to the Security Rule. ePHI is often accessed via organizational resources (e.g., assets, services, workflows, network accounts, etc.). Regulated entities may find value in the following materials to protect organizational data and the resources that store and access ePHI.

- **Zero Trust Architecture** [SP 800-207] – Presents an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. Zero trust focuses on protecting resources (e.g., ePHI).
- **Digital Identity Guidelines** [SP 800-63-3] – Provides technical requirements for federal agencies implementing digital identity services and defines technical requirements in the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions.
- **Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations** [SP 800-52] – Provides guidance on the selection and configuration of TLS protocol implementations while making effective use of Federal Information Processing Standards (FIPS) and NIST-recommended cryptographic algorithms.
- **Trustworthy Email** [SP 800-177] – Gives recommendations and guidelines for enhancing trust in email.
- **Managing the Security of Information Exchanges** [SP 800-47] – Provides guidance on identifying information exchanges, considerations for protecting exchanged information, and the agreements needed to help manage protection of the exchanged information.

Incident Handling/Response: At some point, every organization is going to experience a cybersecurity incident. The resources in this section assist regulated entities in planning for incidents and properly handling those that threaten ePHI.

- **Health Industry Cybersecurity Tactical Crisis Response Guide (HIC-TCR)** – Advises health providers on tactical response activities for managing the cybersecurity threats that can occur during an emergency.

- **Healthcare System Cybersecurity Readiness & Response Considerations** – Helps healthcare facilities and the systems they may be a part of understand the roles and responsibilities of stakeholders before, during, and after a cyber incident
- **OCR Cyber Attack Checklist** – Explains the steps for a HIPAA-covered entity or its business associate to take in response to a cyber-related security incident.
- **Cyber Attack Quick Response Infographic** – Illustrates the steps for a HIPAA-covered entity or business associate to take in response to a cyber-related security incident.
- **Best Practices for Victim Response and Reporting of Cyber Incidents** – Provides planning and response guidance based on lessons learned by federal prosecutors while handling cyber investigations and prosecutions. The authors drafted the document with smaller organizations in mind, but larger organizations should also find it useful.
- **Healthcare Organization and Hospital Discussion Guide for Cybersecurity** – Supports and enhances healthcare organizations and hospitals in addressing cybersecurity. Specifically, this document is intended for personnel whose job responsibilities include cybersecurity preparedness and response planning.
- **Guide for Cybersecurity Event Recovery** [SP 800-184] – Provides tactical and strategic guidance regarding the planning, playbook developing, testing, and improvement of recovery planning. It also provides an example scenario that demonstrates guidance and informative metrics that may be helpful for improving the resilience of information systems.
- **Computer Security Incident Handling Guide** [SP 800-61] – Provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident.
- **Cyber Storm: Securing Cyber Space** – Provides the framework for the most extensive government-sponsored cybersecurity exercise of its kind. The exercise series brings together the public and private sectors to simulate the discovery of and response to a significant cyber incident impacting the Nation's critical infrastructure.

Equipment and Data Loss: ePHI can be put at risk due to loss of organizational equipment or data. These resources provide regulated entities with the information needed to prevent the loss of equipment or data and to mitigate the effects of loss.

- **HICP Fact Sheet – Loss or Theft of Equipment or Data** – Provides information and guidance on mitigating the loss or theft of equipment or data.
- **HICP Threat Slides – Loss or Theft of Equipment or Data** – Provides information and guidance on mitigating the loss or theft of equipment or data.
- **HICP Fact Sheet – Insider, Accidental, or Intentional Data Loss** – Provides information and guidance on mitigating data loss.
- **HICP Threat Slides – Insider, Accidental, or Intentional Data Loss** – Provides information and guidance on mitigating data loss.
- **Guidelines for Media Sanitization** [SP 800-88] – Assists organizations and system owners in making practical sanitization decisions based on the confidentiality categorization of their information.

Contingency Planning: Information systems are vital elements in most business processes. For regulated entities, these systems help to store, process, and transmit ePHI. It is critical for the

services provided by these systems to operate effectively without excessive interruption. Contingency planning supports this requirement by enabling the recovery of systems following disruptions. Regulated entities may find these resources helpful in creating and maintaining contingency plans.

- **Plan A… B… Contingency Plan!** – Provides foundational information about contingency plans and what is required by HIPAA.
- **Contingency Planning Guide for Federal Information Systems** [SP 800-34] – Provides guidance to help personnel evaluate information systems and operations to determine contingency planning requirements and priorities. While written for the Federal Government, the content in this publication could also assist other regulated entities.
- **Healthcare COOP and Recovery Planning** – Includes a collection of resources, ideas, templates, references, and hyperlinks to additional information relating to Healthcare Continuity of Operations (COOP) and Healthcare Disaster Recovery.
- **Business Impact Analysis (BIA) Template** – Assists regulated entities in performing a business impact analysis (BIA) on an information system. The template is meant only as a basic guide and may not apply equally to all systems. Modify this template or the general BIA approach as required to best accommodate a specific system.
- **Contingency Planning: Low Impact System Template** – Provides a sample template to address NIST [SP 800-53] security controls from the Contingency Planning family for a low impact information system. The template provided is a guide and may be customized as necessary to best fit the system or organizational requirements for contingency planning.
- **Contingency Planning: Moderate Impact System Template** – Provides a sample template to address NIST [SP 800-53] security controls from the Contingency Planning family for a moderate impact information system. The template provided is a guide and may be customized as necessary to best fit the system or organizational requirements for contingency planning.
- **Contingency Planning: High Impact System Template** – Provides a sample template to address NIST [SP 800-53] security controls from the Contingency Planning family for a high impact information system. The template provided is a guide and may be customized as necessary to best fit the system or organizational requirements for contingency planning.

Supply Chain: Organizations obtain many products and services from third parties that can help in the protection of ePHI. However, regulated entities need to ensure the security of these products and services.

- **Health Industry Cybersecurity Supply Chain Risk Management Guide – Version 2 (HIC-SCRiM-v2)** – Provides a toolkit for small to mid-sized healthcare institutions to better ensure the security of the products and services they procure through an enterprise supply chain cybersecurity risk management program.
- **Key Practices in Cyber Supply Chain Risk Management: Observations from Industry** [IR 8276] – Provides the ever-increasing community of digital businesses a set

of key practices that any organization can use to manage the cybersecurity risks associated with their supply chains.

- **Supply Chain Risk Management Practices for Federal Information Systems and Organizations** [SP 800-161] – Provides guidance to federal agencies on identifying, assessing, and mitigating information and communications technology (ICT) supply chain risks at all levels of their organizations. Non-federal organizations may also find the guidance useful.

Information Sharing: Regulated entities may find benefits in both the sharing and receiving of information related to cybersecurity and the protection of ePHI. These resources can assist regulated entities in setting up and maintaining organizational information sharing programs.

- **Health Industry Cybersecurity Information Sharing Best Practices (HIC-ISBP)** – Explains best practices for how healthcare organizations can set up and manage cyber threat information-sharing programs for their enterprise.
- **Health Industry Cybersecurity Matrix of Information Sharing Organizations (HIC-MISO)** – Identifies many of the cybersecurity information-sharing organizations and their key services, as health organizations are beginning to understand the importance of cybersecurity information sharing and implementing information-sharing systems.
- **Guide to Cyber Threat Information Sharing** [SP 800-150] – Helps organizations establish information-sharing goals, identify cyber threat information sources, scope information-sharing activities, develop rules that control the publication and distribution of threat information, engage with existing sharing communities, and make effective use of threat information in support of the organization's overall cybersecurity practices.

Access Control/Secure Remote Access: To protect ePHI, regulated entities need to ensure proper access control – both internal to the organization and remote access – to ePHI. The resources in this section can help regulated entities secure access to ePHI.

- **Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security** [SP 800-46] – Provides information on security considerations for several types of remote access solutions and makes recommendations for securing a variety of telework, remote access, and BYOD technologies as well as creating related security policies.
- **User's Guide to Telework and Bring Your Own Device (BYOD) Security** [SP 800-114] – Provides recommendations for securing BYOD devices used for teleworking and remote access, as well as those directly attached to the enterprise's own networks.
- **Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions** – Summarizes key concepts and recommendations related to telework and remote access solutions.
- **Utilizing Two-Factor Authentication** – Describes two-factor authentication, a process in which a user must provide two different types of information to gain access to an account or system.
- **Hardening Remote Access VPN** – Provides guidance on hardening virtual private network (VPN) services via an information sheet jointly issued by the National Security Agency (NSA) and CISA.

- **Guide to SSL VPNs** [SP 800-113] – Assists organizations in understanding Secure Sockets Layer (SSL) VPN technologies and makes recommendations for designing, implementing, configuring, securing, monitoring, and maintaining SSL VPN solutions.
- **Guide to IPsec VPNs** [SP 800-77] – Provides practical guidance to organizations on implementing security services based on Internet Protocol Security (IPsec) so that they can mitigate the risks associated with transmitting sensitive information across networks.

Telework: Many organizational personnel work remotely and/or telework. To protect ePHI, regulated entities need to ensure that workers are securely connecting to organizational resources. The resources in this section may help regulated entities in securing organizational telework.

- **12 Tips for Safe Teleworking from HICP** – Details 12 tips that can be implemented from an organization and from home to help fight cyber attacks while teleworking.
- **Telework Essentials Toolkit** – Assists business leaders, IT staff, and end users in developing a secure telework environment through simple, actionable recommendations. The Toolkit provides three personalized modules for executive leaders, IT professionals, and teleworkers.
- **Management Checklist for Teleworking Surge During COVID-19 Response** – Serves as a quick reference for healthcare enterprise management to consider important factors in a teleworking strategy that minimizes downtime and latency while supporting patient care, operational and IT security, and supply chain resilience.
- **User's Guide to Telework and Bring Your Own Device (BYOD) Security** [SP 800-114] – Provides recommendations for securing BYOD devices used for teleworking and remote access, as well as those directly attached to the enterprise's own networks.
- **Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security** [SP 800-46] – Provides information on security considerations for several types of remote access solutions and makes recommendations for securing a variety of telework, remote access, and BYOD technologies as well as creating related security policies.
- **Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions** – Summarizes key concepts and recommendations related to telework and remote access solutions.

Cybersecurity Workforce: A properly skilled and knowledgeable workforce is essential to meeting organizational missions and protecting ePHI. Regulated entities can reference this resource in developing their workforce.

- **Workforce Framework for Cybersecurity (NICE Framework)** – Provides a set of building blocks for describing the tasks, knowledge, and skills that are needed by individuals and teams to perform cybersecurity work. Through these building blocks, the National Initiative for Cybersecurity Education (NICE) Framework enables organizations to develop their workforces to perform cybersecurity work, and it helps learners explore cybersecurity work and engage in appropriate learning activities to develop their knowledge and skills.