DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 160 and 164

RIN 0945–AA22

HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information

AGENCY: Office for Civil Rights (OCR), Office of the Secretary, Department of Health and Human Services.

ACTION: Notice of proposed rulemaking; notice of Tribal consultation.

SUMMARY: The Department of Health and Human Services (HHS or ''Department'') is issuing this notice of proposed rulemaking (NPRM) to solicit comment on its proposal to modify the Security Standards for the Protection of Electronic Protected Health Information (''Security Rule'') under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). The proposed modifications would revise existing standards to better protect the confidentiality, integrity, and availability of electronic protected health information (ePHI). The proposals in this NPRM would increase the cybersecurity for ePHI by revising the Security Rule to address: changes in the environment in which health care is provided; significant increases in breaches and cyberattacks; common deficiencies the Office for Civil Rights has observed in investigations into Security Rule compliance by covered entities and their business associates (collectively, ''regulated entities''); other cybersecurity guidelines, best practices, methodologies, procedures, and processes; and court decisions that affect enforcement of the Security Rule.

DATES:

Comments: Submit comments on or before March 7, 2025.

Meeting: Pursuant to Executive Order 13175, Consultation and Coordination with Indian Tribal Governments, the Department of Health and Human Services' Tribal Consultation Policy, and the Department's Plan for Implementing Executive Order 13175, the Office for Civil Rights solicits input from Tribal officials as the Department develops the modifications to the HIPAA Security Rule at 45 CFR part 160 and subparts A and C of 45 CFR part 164. The Tribal consultation meeting will be held on February 6, 2025, at 2 p.m. to 3:30 p.m. eastern time.

ADDRESSES: You may submit comments, identified by RIN Number 0945–AA22, by any of the following methods. Please do not submit duplicate comments.

- *Federal eRulemaking Portal:* You may submit electronic comments at *https://www.regulations.gov* by searching for the Docket ID number HHS–OCR–0945–AA22. Follow the instructions at *https://www.regulations.gov* for submitting electronic comments. Attachments should be in Microsoft Word or Portable Document Format (PDF).
- *Regular, Express, or Overnight Mail:* You may mail written comments to the following address only: U.S. Department of Health and Human Services, Office for Civil Rights, Attention: HIPAA Security Rule NPRM, Hubert H. Humphrey Building, Room 509F, 200 Independence Avenue SW, Washington, DC 20201. Please allow sufficient time for mailed comments to be timely received in the event of delivery or security delays.

Please note that comments submitted by fax or email and those submitted after the comment period will not be accepted.

Inspection of Public Comments: All comments received by the accepted methods and due date specified above may be posted without change to content to *https://www.regulations.gov,* which may include personal information provided about the commenter, and such posting may occur after the closing of the comment period. However, the Department may redact certain non-substantive content from comments or attachments to comments before posting, including: threats, hate speech, profanity, sensitive health information, graphic images, promotional materials, copyrighted materials, or individually identifiable information about a third-party individual other than the commenter. In addition, comments or material designated as confidential or not to be disclosed to the public will not be accepted. Comments may be redacted or rejected as described above without notice to the commenter, and the Department will not consider in rulemaking any redacted or rejected content that would not be made available to the public as part of the administrative record.

Docket: For complete access to background documents, the plain-language summary of the proposed rule of not more than 100 words in length required by the Providing Accountability Through Transparency Act of 2023, or posted comments, go to *https://www.regulations.gov* and search for Docket ID number HHS–OCR–0945–AA22.

Tribal consultation meeting: To participate in the Tribal consultation meeting, you must register in advance at *https://hhsgov.zoomgov.com/meeting/register/vJItdOyhrjgoHxJWMDxozrxT98yXyCO3lks.*

FOR FURTHER INFORMATION CONTACT: Marissa Gordon-Nguyen at (202) 240–3110 or (800) 537–7697 (TDD), or by email at *OCRPrivacy@hhs.gov.*

SUPPLEMENTARY INFORMATION: The discussion below includes an Executive Summary, a description of relevant statutory and regulatory authority and history, the justification for this proposed regulation, a section-by-section description of the proposed modifications, and a regulatory impact analysis and other required regulatory analyses. The Department solicits public comment on all aspects of the proposed rule. The Department requests that persons commenting on the provisions of the proposed rule label their discussion of any particular provision or topic with a citation to the section of the proposed rule being addressed and identify the particular request for comment being addressed, if applicable.

Table of Contents

I. Executive Summary
- A. Overview
- B. Applicability
- C. Table of Abbreviations/Commonly Used Acronyms in This Document

II. Statutory Authority and Regulatory History
- A. Statutory Authority and History
- 1. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- 2. Health Information Technology for Economic and Clinical Health (HITECH) Act
- B. Regulatory History
- 1. 1998 Security Rule Notice of Proposed Rulemaking
- 2. 2003 Final Rule
- 3. 2009 Delegation of Authority
- 4. 2013 Omnibus Rulemaking

III. Justification for This Proposed Rulemaking
- A. Strong Security Standards Are Essential to Protecting the Confidentiality, Integrity, and Availability of ePHI and Ensuring Quality and Efficiency in the Health Care System
- B. The Health Care Environment Has Changed Since the Security Rule Was Last Revised and Will Continue To Evolve
- C. Regulated Entities' Compliance With the Requirements of the Security Rule Is Inconsistent
- D. It Is Reasonable and Appropriate To Strengthen the Security Rule To Address the Changes in the Health Care Environment and Clarify the Compliance Obligations of Regulated Entities
- 1. Congress and the Department Anticipated That Security Standards

PLEAES NOTE: All highlighting and comments added are by TFS. Comments may contain opinions we have based on our 15 years of experience working with HIPAA Security Rule.

Safeguards Would Evolve To Address Changes in the Health Care Environment
2. NCVHS Believes That the Security Standards Evolve To Address Changes in the Health Care Environment
3. A Strengthened Security Rule Would Continue To Be Flexible and Scalable While Providing Regulated Entities With Greater Clarity
4. Small and Rural Health Care Providers Must Implement Strong Security Measures To Provide Efficient and Effective Health Care
5. A Strengthened Security Rule Is Critical to an Efficient and Effective Health Care System
E. The Secretary Must Develop Standards for the Security of ePHI Because None Have Been Developed by an ANSI-Accredited Standard Setting Organization
F. Section-by-Section Description of the Proposed Amendments to the Security Rule
A. Section 160.103—Definitions
1. Current Provision
2. Issues To Address
3. Proposals
4. Request for Comment
B. Section 164.304—Definitions
1. Clarifying the Definition of ''Access''
2. Clarifying the Definition of ''Administrative Safeguards''
3. Clarifying the Definition of ''Authentication''
4. Clarifying the Definition of ''Availability''
5. Clarifying the Definition of ''Confidentiality''
6. Adding Definitions of ''Deploy'' and ''Implement''
7. Adding a Definition of ''Electronic Information System''
8. Modifying the Definition of ''Information System''
9. Modifying the Definition of ''Malicious software''
10. Adding a Definition of ''Multi-factor Authentication'' (MFA)
11. Clarifying the Definition of ''Password''
12. Clarifying the Definition of ''Physical Safeguards''
13. Adding a Definition of ''Relevant Electronic Information System''
14. Adding a Definition of ''Risk''
15. Clarifying the Definitions of ''Security or Security Measures'' and ''Security Incident''
16. Adding Definitions of ''Technical Controls''
17. Modifying the Definition of ''Technical Safeguards''
18. Adding a Definition of ''Technology Asset''
19. Adding a Definition of ''Threat''
20. Clarifying the Definition of ''User''
21. Adding a Definition of ''Vulnerability''
22. Clarifying the Definition of ''Workstation''
23. Request for Comment
C. Section 164.306—Security Standards: General Rules
1. Current Provisions
2. Issues To Address
3. Proposals
4. Request for Comment
D. Section 164.308—Administrative Safeguards
1. Current Provisions
2. Issues To Address
3. Proposals
4. Request for Comment
E. Section 164.310—Physical Safeguards
1. Current Provisions
2. Issues To Address
3. Proposals
4. Request for Comment
F. Section 164.312—Technical Safeguards
1. Current Provisions
2. Issues To Address
3. Proposals
4. Request for Comment
G. Section 164.314—Organizational Requirements
1. Section 164.314(a)(1)—Standard: Business Associate Contracts or Other Arrangements
2. Section 164.314(b)(1)—Standard: Requirements for Group Health Plans
3. Request for Comment
H. Section 164.316—Documentation Requirements
1. Current Provisions
2. Issues To Address
3. Proposals
4. Request for Comment
I. Section 164.318—Transition Provisions
1. Current Provisions and Issues To Address
2. Proposal
3. Request for Comment
J. Section 164.320—Severability
K. New and Emerging Technologies Request for Information
1. Quantum Computing
2. Artificial Intelligence (AI)
3. Virtual and Augmented Reality (VR and AR)
4. Request for Comment
V. Regulatory Impact Analysis
A. Executive Order 12866 and Related Executive Orders on Regulatory Review
1. Summary of Costs and Benefits
2. Baseline Conditions
3. Costs of the Proposed Rule
4. Benefits of the Proposed Rule
5. Comparison of Benefits and Costs
B. Regulatory Alternatives to the Proposed Rule
C. Regulatory Flexibility Act—Small Entity Analysis
D. Executive Order 13132—Federalism
E. Assessment of Federal Regulation and Policies on Families
F. Paperwork Reduction Act of 1995
1. Explanation of Estimated Annualized Burden Hours

I. Executive Summary

A. Overview

In this notice of proposed rulemaking (NPRM), the Department of Health and Human Services (HHS or ''Department'') proposes modifications to the Security Standards for the Protection of Electronic Protected Health Information (''Security Rule''), issued pursuant to section 262(a) of the Administrative Simplification provisions of title II, subtitle F, of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[1] The Security Rule[2] is one of several rules, collectively known as the HIPAA Rules,[3] that protect the privacy and security of individuals' protected health information[4] (PHI), which is individually identifiable health information[5] (IIHI) transmitted by or maintained in electronic media or any other form or medium, with certain exceptions.[6] The Security Rule applies only to electronic PHI (ePHI), which is IIHI that is transmitted by or maintained in electronic media.[7]

The Security Rule was initially published in 2003 and most recently revised in 2013.[8] Since its publication, there have been significant changes to the environment in which health care is provided and how the health care industry operates. Today, cybersecurity is a concern that touches nearly every facet of modern health care, certainly more than it did in 2003 or even 2013.

[1] Subtitle F of title II of HIPAA (Pub. L. 104–191, 110 Stat. 1936 (Aug. 21, 1996)) added a new part C to title XI of the Social Security Act of 1935 (SSA), Public Law 74–271, 49 Stat. 620 (Aug. 14, 1935), (*see* sections 1171–1179 of the SSA (codified at 42 U.S.C. 1320d–1320d–8)), as well as promulgating section 264 of HIPAA (codified at 42 U.S.C. 1320d–2 note), which authorizes the Secretary to promulgate regulations with respect to the privacy of individually identifiable health information. The Privacy Rule has subsequently been amended pursuant to the Genetic Information Nondiscrimination Act of 2008, title I, section 105, Public Law 110–233, 122 Stat. 881 (May 21, 2008) (codified at 42 U.S.C. 2000ff), and the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, Public Law 111–5, 123 Stat. 226 (Feb. 17, 2009) (codified at 42 U.S.C. 139w–4(0)(2)).

[2] 45 CFR part 160 subparts A and C of 45 CFR part 164. For a history of the Security Rule, *see* section II.B, ''Regulatory History.''

[3] *See also* the HIPAA Privacy Rule, 45 CFR part 160 and subparts A and E of 45 CFR part 164; HIPAA Breach Notification Rule, 45 CFR part 164, subpart D; and the HIPAA Enforcement Rule, 45 CFR part 160, subparts C through E.

[4] 45 CFR 160.103 (definition of ''Protected health information'').

[5] 45 CFR 160.103 (definition of ''Individually identifiable health information'').

[6] At times throughout this NPRM, the Department uses the terms ''health information'' or ''individuals' health information'' to refer generically to health information pertaining to an individual or individuals. In contrast, the Department's use of the term ''IIHI'' refers to a category of health information defined in HIPAA, and ''PHI'' is used to refer specifically to a category of IIHI that is defined by and subject to the requirements of the HIPAA Rules. The HIPAA Rules exclude from the definition of PHI: IIHI in employment records held by a covered entity in its role as employer; IIHI in education records and certain treatment records covered by the Family Educational Rights and Privacy Act (codified at 20 U.S.C. 1232g); and IIHI regarding a person who has been deceased for more than 50 years. 45 CFR 160.103 (definition of ''Protected health information'').

[7] 45 CFR 160.103 (definition of ''Electronic protected health information'').

[8] *See* 68 FR 8334 (Feb. 20, 2003) and 78 FR 5566 (Jan. 25, 2013).

Almost every stage of modern health care relies on stable and secure computer and network technologies, including, but not limited to, the following: appointment scheduling, prescription orders, telehealth visits, medical devices, patient records, medical and pharmacy claims submissions and billing, insurance coverage verifications, payroll, facilities access and management, internal and external communications, and clinician resources. These tools and technologies are an integral part of the modern health care system, but they also present opportunities for bad actors to cause harm through hacking, ransomware, and other means. Covered entities and business associates (collectively, ''regulated entities'') may also experience malfunctions and inadvertent errors that threaten the confidentiality, integrity, or availability of ePHI. Thus, cyberattacks, malfunctions, and inadvertent errors can negatively affect the provision of health care, as well as the efficiency and effectiveness of the health care system.

As discussed in greater detail below, in recent years, there has been an alarming growth in the number of breaches affecting 500 or more individuals reported to the Department, the overall number of individuals affected by such breaches, and the rampant escalation of cyberattacks using hacking and ransomware. The Department is concerned by the increasing numbers of breaches and other cybersecurity incidents experienced by regulated entities. We [9] are also increasingly concerned by the upward trend in the numbers of individuals affected by such incidents and the magnitude of the potential harms from such incidents.[10]

In recognition of those potential harms and the health care sector's importance to the economy and security of the U.S., the President has designated ''Healthcare and Public Health'' as a critical infrastructure sector [11] and the Department as the Sector Risk Management Agency (SRMA).[12] In addition, to address concerns about the increasing level of cybercrime, the President has charged Federal agencies with ''establishing and implementing minimum requirements for risk management'' and robustly enforcing those requirements and Federal laws to help manage that risk.[13] We believe that a comprehensive and updated Security Rule is critical to accomplishing these directives and to the Department's effectiveness as the SRMA for the Healthcare and Public Health sector.

In further recognition of these concerns, States have promulgated or are in the process of promulgating regulations that would require the adoption of certain standards or measures for the protection of sensitive information, such as PHI.[14] While these proposed regulations may contain helpful guidance for regulated entities, none specifically focus on ensuring the security of ePHI and the information systems that create, receive, maintain, or transmit ePHI. Additionally, a patchwork of State-specific laws may create difficulties for regulated entities that are located or operate in multiple States. Several entities, including Federal agencies, have published and maintained guidelines, best practices, methodologies, procedures, and processes for protecting the security of sensitive information, including PHI. Some examples of these resources include the National Institute of Standards and Technology's (NIST's) ''Cybersecurity Framework,'' [15] the HHS 405(d) Program's ''Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients,'' [16] the Federal Trade Commission's (FTC's) ''Start with Security: A Guide for Business,'' [17] and the Department's ''Cybersecurity Performance Goals'' (CPGs).[18] We believe that the proliferation of such documents in recent years has been helpful, and we have considered them in the development of this NPRM. However, in light of the increasing number and sophistication of cybersecurity incidents, we do not believe that these documents are sufficiently instructive for regulated entities to help improve their compliance with the Security Rule.

Under its statutory authority to administer and enforce the HIPAA Rules, the Department modifies the HIPAA Rules as needed, but does not modify a standard or implementation specification more than once every 12 months.[19] The Department makes the determination that such modifications may be needed using information it receives on an ongoing basis—from the Department's Federal advisory committee on HIPAA, the public, regulated entities, media reports, and its own analysis of the state of privacy and security for IIHI. As referenced above, and discussed in greater detail below, while the Department believes that the Security Rule generally continues to accomplish the goals of HIPAA,[20] we believe that it would be appropriate to consider modifying the Security Rule to address the following:

- Significant changes in technology.
- Changes in breach trends and cyberattacks.
- HHS' Office for Civil Rights' (OCR's) enforcement experience.
- Other guidelines, best practices, methodologies, procedures, and processes for protecting ePHI.
- Court decisions that affect enforcement of the Security Rule.

B. Applicability

The effective date of a final rule would be 60 days after publication.[21] Regulated entities would have until the ''compliance date'' to establish and implement policies, procedures, and practices to achieve compliance with any new or modified standards.

---

[9] In this NPRM, ''we'' and ''our'' denote the Department.

[10] *See* ''Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,'' Office for Civil Rights, U.S. Department of Health and Human Services, *https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.*

[11] Presidential Memorandum on National Security Memorandum on Critical Infrastructure Security and Resilience, National Security Memorandum/NSM–22, The White House (Apr. 30, 2024), *https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/* (''Critical infrastructure comprises the physical and virtual assets and systems so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, or national public health or safety.'').

[12] *Id.* (charging an SRMA with serving as the primary Federal liaison to their designated critical infrastructure and ''conduct[ing] sector-specific risk management and resilience activities'').

[13] *Id.*

[14] *See, e.g.,* ''New York State Register,'' 46 N.Y. Reg. 7–10, Division of Administrative Rules, New York State Department of State (Oct. 2, 2024), *https://dos.ny.gov/system/files/documents/2024/10/100224.pdf;* ''Invitation for Preliminary Comments on Proposed Rulemaking: Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking,'' California Privacy Protection Agency (Feb. 10, 2023), *https://cppa.ca.gov/regulations/pdf/invitation_for_comments_pr_02-2023.pdf; see also* Cal. Civ. Code Section 1798.185.

[15] ''The NIST Cybersecurity Framework (CSF) 2.0,'' National Institute of Standards and Technology, U.S. Department of Commerce (Feb. 26, 2024), *https://doi.org/10.6028/NIST.CSWP.29.*

[16] ''Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients,'' U.S. Department of Health and Human Services and the Healthcare & Public Health Sector Coordinating Council (2023), *https://405d.hhs.gov/Documents/HICP-Main-508.pdf.*

[17] ''Start with Security: A Guide for Business,'' Federal Trade Commission (Aug. 2023), *https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf.*

[18] ''Cybersecurity Performance Goals,'' U.S. Department of Health and Human Services (Jan. 2024), *https://hphcyber.hhs.gov/performance-goals.html.*

[19] Sec. 1174(b)(1) of the SSA; 45 CFR 160.104.

[20] *See* sec. 261 of Public Law 104–191, 110 Stat. 1936 (codified at 42 U.S.C. 1320d note).

[21] *See* ''A Guide to the Rulemaking Process,'' Office of the Federal Register (2011), p. 8, *https://www.federalregister.gov/uploads/2011/01/the_rulemaking_process.pdf.*

Regulated entities would be permitted to comply earlier than the compliance date, but the Department would not take action against them for noncompliance with the proposed changes that occurs before the compliance date. Except as otherwise provided, 45 CFR 160.105 provides that regulated entities must comply with the applicable new or modified standards or implementation specifications no later than 180 days from the effective date of any such change. The Department has previously noted that the 180-day general compliance period for new or modified standards would not apply where a different compliance period is provided in the regulation for one or more provisions.[22] However, the compliance period cannot be less than the statutory minimum of 180 days.[23]

While we recognize that we are proposing to substantially revise the regulatory text, the Department believes that most of the existing Security Rule's obligations for regulated entities would not be substantially changed by the proposed modifications. Instead, the proposed modifications would explicitly codify those activities that are critical to protecting the security of ePHI as requirements and provide greater detail for such requirements in the regulatory text. For example, regulated entities are already required to conduct an accurate and thorough risk analysis. While not specified in the regulatory text of the Security Rule, an accurate and thorough risk analysis requires a regulated entity to perform an inventory of its technology assets, determine how ePHI moves through its information systems, and identify the locations within its information systems (or components thereof) where ePHI may be created, received, maintained, or transmitted. Applying such an approach protects ePHI across all phases of the data lifecycle consistent with the purpose of the Security Rule. The proposals to require a regulated entity to inventory its technology assets and map the movement of ePHI through its information systems would illuminate considerations to be included in the regulated entity's risk analysis.

As another example, implementing a mechanism to encrypt ePHI is an addressable implementation specification under the standard for access control at 45 CFR 164.312(a)(2)(iv). Under the existing Security Rule, a regulated entity must assess whether encryption is a reasonable and appropriate safeguard in its environment, when analyzed with reference to its likely contribution to protecting ePHI, and implement encryption if reasonable and appropriate.[24] If encryption is not reasonable and appropriate, a regulated entity must document why it would not be reasonable and appropriate for it to implement the safeguard and must implement an equivalent alternative measure if reasonable and appropriate.[25] As discussed in greater detail below, encryption is built into most software today, and where it is not, there are affordable and easily implemented solutions that can encrypt sensitive information. Thus, it generally would be reasonable and appropriate for regulated entities to implement a mechanism to encrypt ePHI, and regulated entities should already have done so in most circumstances. By expressly requiring regulated entities to encrypt ePHI, with limited exceptions, the Department's proposal would reflect our expectations in the current cybersecurity environment and eliminate the need for regulated entities to perform an analysis of whether encryption is reasonable and appropriate.

Thus, most of the modifications we are proposing would provide regulated entities with greater clarity and specificity regarding how to fulfill their obligations and the Department's expectations.

Accordingly, we do not believe that the proposed rule would pose unique implementation challenges that would justify an extended compliance period (*i.e.,* a period longer than the standard 180 days provided in 45 CFR 160.105). Further, the Department believes that adherence to the standard compliance period is necessary to timely address the circumstances described in this NPRM. Thus, the Department proposes to apply the standard compliance date of 180 days after the effective date of a final rule.[26]

To help reduce administrative burdens on regulated entities, the Department proposes to add a provision at 45 CFR 164.318 affording regulated entities a transition period (beyond the 180-day compliance period) to modify business associate contracts (herein referred to as ''business associate agreements'') or other written arrangements[27] that would qualify for the longer transition period, as discussed further below.

The Department seeks comment on the proposed compliance period and transition period.

C. Table of Abbreviations/Commonly Used Acronyms in This Document

As used in this preamble, the following terms and abbreviations have the meanings noted below.

Term	Meaning
AI	Artificial Intelligence.
ANSI	American National Standards Institute.
AR	Augmented Reality.
ARRA	American Recovery and Reinvestment Act of 2009.
ASTP/ONC	Assistant Secretary for Technology Policy and Office of the National Coordinator for Health Information Technology.
CISA	Cybersecurity & Infrastructure Security Agency.
CMS	Centers for Medicare & Medicaid Services.
CPG	Cybersecurity Performance Goal.
Department or HHS	Department of Health and Human Services.
EHR	Electronic Health Record.
E.O.	Executive Order.
ePHI	Electronic Protected Health Information.
FDA	Food & Drug Administration.
FISMA	Federal Information Security Modernization Act.
FTC	Federal Trade Commission.
Health IT	Health Information Technology.

[22] *See* 78 FR 5566, 5569 (Jan. 25, 2013).

[23] *See* 42 U.S.C. 1320d–4(b)(2).

[24] 45 CFR 164.306(d)(3)(i) and (d)(3)(ii)(A).

[25] 45 CFR 164.306(d)(3)(ii)(B).

[26] *See* 45 CFR 160.104(c)(1), which requires the Secretary to provide at least a 180-day period for regulated entities to comply with modifications to standards and implementation specifications in the HIPAA Rules.

[27] 45 CFR 164.314(a)(1).

Term	Meaning
HIPAA	Health Insurance Portability and Accountability Act of 1996.
HITECH Act	Health Information Technology for Economic and Clinical Health Act of 2009.
ICR	Information Collection Request.
IIHI	Individually Identifiable Health Information.
IT	Information Technology.
MFA	Multi-factor Authentication.
NAICS	North American Industry Classification System.
NCVHS	National Committee on Vital and Health Statistics.
NIST	National Institute of Standards and Technology.
NPRM	Notice of Proposed Rulemaking.
OCR	Office for Civil Rights.
OMB	Office of Management and Budget.
ONC	Office of the National Coordinator for Health Information Technology.
PHI	Protected Health Information.
PRA	Paperwork Reduction Act of 1995.
PSAO	Pharmacy Services Administration Organizations.
RFA	Regulatory Flexibility Act.
RIA	Regulatory Impact Analysis.
SBA	Small Business Administration.
SRMA	Sector Risk Management Agency.
SSA	Social Security Act of 1935.
UMRA	Unfunded Mandates Reform Act of 1995.
VR	Virtual Reality.

II. Statutory Authority and Regulatory History

A. Statutory Authority and History

1. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

In 1996, Congress enacted HIPAA [28] to reform the health care delivery system to ''improve portability and continuity of health insurance coverage in the group and individual markets'' [29] and ''to simplify the administration of health insurance.'' [30] Through subtitle F of HIPAA, Congress amended title XI of the Social Security Act of 1935 (SSA) by adding part C, entitled ''Administrative Simplification.'' [31] A primary purpose of part C is to improve the Medicare and Medicaid programs and ''the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of uniform standards and requirements for the electronic transmission of certain health information.'' [32]

Congress recognized that the development of a health information system that enabled the electronic transmission of IIHI as required by HIPAA would pose risks to the privacy of confidential health information and viewed individual privacy, confidentiality, and data security as critical to support the shift from a paper-based recordkeeping system for health information to a digital one.[33] Congress intended for the law to enhance individuals' trust in health care providers, which required that the law provide additional protection for the confidentiality of IIHI. As described by a Member of Congress at the time of the law's passage: ''[t]his standardization, however, accelerates the creation of large databases containing personally identifiable information. All this information is transmitted over electronic networks. We need to be very careful about how safe and secure that information is from prying eyes. Some of it may be extremely sensitive and could be used in a malicious or discriminatory manner.'' [34] Moreover, Congress considered that health care reform required an approach that would not compromise privacy as health information became more accessible.[35]

Congress applied the Administrative Simplification provisions directly to three types of persons referred to in regulation as covered entities: health plans, health care clearinghouses, and health care providers who transmit information electronically in connection with a transaction for which HHS has adopted a standard.[36] Under HIPAA, covered entities are required to maintain reasonable and appropriate administrative, physical, and technical safeguards [37] to: (1) ensure the integrity and confidentiality of information; [38] (2) protect against any reasonably anticipated threats or hazards to the security or integrity of the information and unauthorized uses or disclosures of the information; [39] and (3) otherwise ensure compliance with HIPAA by the officers and employees of covered entities.[40]

HIPAA required the Secretary to adopt uniform standards ''to enable health information to be exchanged electronically.'' [41] Congress also directed the Secretary to, among other things, adopt standards for the security of IIHI.[42] The statute also directed the Secretary to adopt initial security standards within 18 months of its

[28] Public Law 104–191, 110 Stat. 1936 (Aug. 21, 1996) (codified at 42 U.S.C. 201 note).

[29] *See* H.R. Rep. No. 104–496, at 66–67 (1996).

[30] Public Law 104–191, 110 Stat. 1936 (Aug. 21, 1996).

[31] Sec. 262(a) of Public Law 104–191, 110 Stat. 2021 (Aug. 21, 1996) (codified at 42 U.S.C. 1320d).

[32] Sec. 261 of Public Law 104–191, 110 Stat. 2021 (Aug. 21, 1996), as amended by sec. 1104(a) of Public Law 111–148, 124 Stat. 146 (Mar. 23, 2010) (codified at 42 U.S.C. 1320d note).

[33] On a resolution waiving points of order against the Conference Report to H.R. 3103, members debated an ''erosion of privacy'' balanced against the administrative simplification provisions. Thus, from HIPAA's inception, privacy has been a central concern to be addressed as legislative changes eased disclosures of PHI. *See* 142 Cong. Rec. H9777 and H9780.

[34] 142 Cong. Rec. S9515–16 (daily ed. Aug. 2, 1996) (statement of Sen. Simon).

[35] *See* H.R. Rep. No. 104–496 Part 1, at 99–100 (Mar. 25, 1996).

[36] *See* sec. 262(a) of Public Law 104–191, 110 Stat. 2021, adding section 1172 to the SSA (codified at 42 U.S.C. 1320d–1); *see also* section 13404 of the American Recovery and Reinvestment Act (ARRA) of 2009, Public Law 111–5, 123 Stat. 115 (Feb. 17, 2009) (codified at 42 U.S.C. 17934) (applying privacy provisions and penalties to business associates of covered entities). The Department codified the term ''covered entity'' and defined it using these three categories of persons. 45 CFR 164.103.

[37] 42 U.S.C. 1320d–2(d)(2).

[38] 42 U.S.C. 1320d–2(d)(2)(A).

[39] 42 U.S.C. 1320d–2(d)(2)(B).

[40] 42 U.S.C. 1320d–2(d)(2)(C).

[41] Sec. 262(a) of Public Law 104–191, 110 Stat. 2024, adding sec. 1173(a) (codified at 42 U.S.C. 1320d–2(a)(1)).

[42] Sec. 262(a) of Public Law 104–191, 110 Stat. 2025, adding sec. 1173(d) (codified at 42 U.S.C. 1320d–2(d)).

enactment.[43] In adopting security standards for health information, HIPAA requires the Secretary to consider all of the following: [44]

- The technical capabilities of record systems used to maintain health information.
- The costs of security measures.
- Training for persons who have access to health information.
- The value of audit trails in computerized record systems.
- The needs and capabilities of small health care providers and rural health care providers.[45]

Congress contemplated that the Department's rulemaking authorities under HIPAA would not be static. In fact, Congress specifically built in a mechanism to adapt such regulations as technology and health care evolve, directing the Secretary to review and adopt modifications to the Administrative Simplification standards, including the security standards, as determined appropriate, but not more frequently than once every 12 months.[46] That statutory directive complements the Secretary's general rulemaking authority to make and publish such rules and regulations as may be necessary to the efficient administration of the functions with which the Secretary is charged.[47] The Secretary may adopt either a standard developed, adopted, or modified by a standard setting organization that relates to a standard that the Secretary is authorized or required to adopt under the Administrative Simplification provisions, or a standard that is different if the different standard will substantially reduce administrative costs to health care providers and health plans.[48] If no standard has been adopted by any standard setting organization, the Secretary shall rely on the recommendations of the National Committee on Vital and Health Statistics (NCVHS) and consult with Federal and State agencies and private organizations.[49]

[43] Sec. 262(a) of Public Law 104–191, 110 Stat. 2026, adding sec. 1174(a) (codified at 42 U.S.C. 1320d–3(a)).

[44] Sec. 262(a) of Public Law 104–191, 110 Stat. 2025, adding sec. 1173(d)(1) (codified at 42 U.S.C. 1320d–2(d)(1)).

[45] *Id.*

[46] Sec. 262(a) of Public Law 104–191, 110 Stat. 2026, adding sec. 1174(b)(1) (codified at 42 U.S.C. 1320d–3).

[47] Sec. 1102 of the SSA (codified at 42 U.S.C. 1302).

[48] Sec. 262(a) of Public Law 104–191, 110 Stat. 2023, adding sec. 1172 (codified at 42 U.S.C. 1320d–1).

[49] *Id.*

2. Health Information Technology for Economic and Clinical Health (HITECH) Act

On February 17, 2009, Congress enacted the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act), part of the American Recovery and Reinvestment Act of 2009 (ARRA),[50] promoting the nationwide adoption and standardization of health information technology (health IT) to support the electronic sharing of clinical data. The HITECH Act created financial incentives for health IT use among health care practitioners by providing funding for investing in health IT infrastructure, purchasing certified electronic health records (EHRs), and training on and the dissemination of best practices to integrate health IT.[51] The Purpose statement of an accompanying House of Representatives report [52] on the Energy and Commerce Recovery and Reinvestment Act [53] recognizes that widespread health IT adoption ''has the potential to ameliorate many of the quality and efficiency problems endemic to our health care system.'' Congress also understood that ''[e]nsuring the privacy and security of electronic health information is critical to the success'' of this immense effort to promote health IT adoption.[54] As a result, the HITECH Act also introduced substantial changes to the HIPAA regulations by mandating stronger safeguards for the privacy and security of ePHI.[55]

The HITECH Act's security requirements focused on safeguarding an individual's health information while allowing covered entities to rapidly adopt new technologies to improve the quality and efficiency of patient care.[56] Specifically, the HITECH Act extends the application of the Security Rule's provisions on administrative, physical, and technical safeguards and documentation requirements to business associates of covered entities, making those business associates subject to civil and criminal liability for violations of the Security Rule.[57] The HITECH Act also requires existing business associate agreements to incorporate new security requirements.[58] Additionally, the HITECH Act requires the Secretary to regularly issue guidance on the most effective and appropriate technical safeguards.[59]

In enacting the HITECH Act, Congress affirmed that the existing HIPAA Rules were to remain in effect to the extent that they are consistent with the HITECH Act and directed the Secretary to revise the HIPAA Rules as necessary for consistency with the HITECH Act.[60] Congress confirmed that the new law was not intended to have any effect on authorities already granted under HIPAA to the Department, including part C of title XI of the SSA.[61] Thus, Congress affirmed the Secretary's ongoing rulemaking authority to modify the Security Rule's standards and implementation specifications as often as every 12 months when appropriate, including to strengthen security protections for IIHI.

In 2021, the HITECH Act was amended to require the HHS Secretary to further encourage regulated entities to bolster their cybersecurity practices.[62] The amendment requires the Department to consider certain recognized security practices of regulated entities when making determinations relating to certain Security Rule compliance and enforcement activities.[63]

B. Regulatory History

The Security Rule requires regulated entities to implement administrative, physical, and technical safeguards to

[50] Title XIII of Division A and title IV of Division B of ARRA of 2009, Public Law 111–5, 123 Stat. 115 (Feb. 17, 2009) (codified at 42 U.S.C. 201 note).

[51] *Id.; see also* Subtitle B of title XIII of the HITECH Act (codified at 42 U.S.C. 17911–17912), 42 U.S.C. 300jj–31–38.

[52] *See* H.R. Rep. No. 111–7, at 74 (2009), accompanying H.R. 629, 111th Cong.

[53] H.R. 629, Energy and Commerce Recovery and Reinvestment Act of 2009, introduced in the House on Jan. 22, 2009, contained nearly identical provisions to subtitle D of the HITECH Act.

[54] C. Stephen Redhead, ''The Health Information Technology for Economic and Clinical Health (HITECH) Act,'' Congressional Research Service, p. 8 (2009), *https://crsreports.congress.gov/product/pdf/R/R40161/9; id.* at 9 (''[Health IT], which generally refers to the use of computer applications in medical practice, is widely viewed as a necessary and vital component of health care reform.'').

[55] Subtitle D of title XIII of the HITECH Act (codified at 42 U.S.C. 17921, 42 U.S.C. 17931–17941, and 42 U.S.C. 17951–17953).

[56] *See* S. Rept. 111–3, 111th Cong. accompanying S. 336, 111th Cong., at 59 (2009).

[57] Sec. 13401 of Public Law 111–5, 123 Stat. 260 (codified at 42 U.S.C. 17931).

[58] Sec. 13401(a) of Public Law 111–5, 123 Stat. 260 (codified at 42 U.S.C. 17931).

[59] Sec. 13401(c) of Public Law 111–5, 123 Stat. 260 (codified at 42 U.S.C. 17931).

[60] Sec. 13421(b) of the HITECH Act (codified at 42 U.S.C. 17951).

[61] Sec. 3009(a)(1)(A) of the PHSA, as added by sec. 13101 of the HITECH Act (codified at 42 U.S.C. 300jj–19(a)(1)).

[62] *See* Public Law 116–321, 134 Stat. 5072, adding sec. 13412 (Jan. 5, 2021) (codified at 42 U.S.C. 17941); *see also* 42 U.S.C. 17931 *et seq.*

[63] *See* Public Law 116–321, 134 Stat. 5072, adding sec. 13412 (Jan. 5, 2021) (codified at 42 U.S.C. 17941); *see also* sec. 13401 of Public Law 111–5, 123 Stat. 260 (codified at 42 U.S.C. 17931) (The HITECH Act adopts the same definition of business associate as the HIPAA Rules.); 45 CFR 160.103 (definition of ''Business associate'').

protect ePHI.[64] Specifically, regulated entities must ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit;[65] protect against reasonably anticipated threats or hazards to the security or integrity of the information[66] and reasonably anticipated impermissible uses or disclosures;[67] and ensure compliance by their workforce.[68]

1. 1998 Security Rule Notice of Proposed Rulemaking

The Administrative Simplification provisions of HIPAA instructed the Secretary to adopt several standards concerning electronic transmission of health information, including those for the security of health information.[69] In accordance with these provisions, the Department published the Security and Electronic Signature Standards; Proposed Rule (''1998 Proposed Rule'') on August 12, 1998.[70]

In support of developing the national standards mandated under HIPAA's Administrative Simplification provisions, the Secretary, with significant input from the health care industry, defined a set of principles for guiding choices for the standards to be adopted by the Secretary.[71] The principles were based on direct specifications in HIPAA and also took the purpose of the law and generally desirable principles into account. Based on this work, the Department proposed that each HIPAA standard should be clear and unambiguous but technology neutral, improve the efficiency and effectiveness of the health care system, meet the needs of covered entities related to ease of use and affordability of adoption, and maintain consistency or alignment with other HIPAA standards adopted by an organization accredited by the American National Standards Institute (ANSI) and using the ANSI process for adopting such standards.[72]

In describing its general approach to the 1998 Proposed Rule, the Department defined the security standard as a set of requirements with implementation features that covered entities must include in their operations to assure the security of individuals' ePHI.[73] The security standard was based on three basic concepts that were derived from the Administrative Simplification provisions of HIPAA and consistent with the characteristics the Department identified as appropriate for all HIPAA Rules.[74] First, the standard should be comprehensive and coordinated to address all aspects of security. Second, it should be scalable, so that it could be effectively implemented by covered entities of all types and sizes. Third, it should not be linked to specific technologies, allowing covered entities the flexibility to make use of future technology advancements.[75]

The 1998 Proposed Rule included four categories of requirements that a covered entity would have to address to safeguard the confidentiality, integrity, and availability of ePHI. They were as follows:

- Administrative procedures.
- Physical safeguards.
- Technical security services.
- Technical mechanisms.

The implementation specifications described some of the requirements in greater detail, based on our determination regarding the level of instruction necessary to implement such requirements.[76] The Department viewed all categories as equally important.[77]

The proposed standard did not address the extent to which a covered entity should implement the specifications.[78] Instead, the Department proposed to require that each covered entity assess its own security needs and risks and devise, implement, and maintain appropriate security to address its business requirements. The Department believed that this approach would leave a significant amount of flexibility for covered entities and balance the needs of securing health data against risk with the economic cost of doing so.[79]

2. 2003 Final Rule

The Department issued the final Security Rule[80] on February 20, 2003 (''2003 Final Rule''). In accordance with the Administrative Simplification provisions of HIPAA, the 2003 Final Rule adopted standards for the security of ePHI to be implemented by covered entities.

The Department reiterated the purposes and guiding principles it articulated in the 1998 Proposed Rule and repeated that the protection of the privacy of information depends in large part on the existence of security measures to protect that information.[81] The Department noted that there were still no standard measures in the health care industry that address all aspects of the security of ePHI while it is being stored or during the exchange of that information between entities.[82] The Department explained that the use of the security standards would improve the Medicare and Medicaid programs, other Federal health programs and private health programs, and the effectiveness and efficiency of the health care industry in general by establishing a level of protection for ePHI.[83]

Provisions of the 2003 Final Rule did not mirror the 1998 Proposed Rule; rather, the Department finalized only certain changes. The Department noted, for example, that to maintain consistency with the use of terms as they appear in the statute and other previously released HIPAA Rules (*i.e.,* the HIPAA Privacy and Transactions Rules), it was changing some terminology from the 1998 Proposed Rule, replacing the terms ''requirement'' with ''standard'' and ''implementation feature'' with ''implementation specification.''[84]

According to the Department, the comments received in response to the 1998 Proposed Rule overwhelmingly validated its basic assumptions that the covered entities were so varied in terms of installed technology, size, resources, and relative risk, that it would be impossible to dictate a specific solution or set of solutions that would be usable by all covered entities.[85] Similarly, we received numerous comments expressing the view that the security standards should not be overly prescriptive because the speed with which technology is evolving could make specific requirements obsolete and might in fact deter technological progress. Accordingly, the Department framed the standards in the 2003 Final Rule in terms that were as generic as possible and that could generally be met through a variety of approaches or technologies.[86] The standards, we

[64] The Security Rule is codified at 45 CFR part 160 and subparts A and C of 45 CFR part 164.

[65] *See* 45 CFR 164.306(a)(1).

[66] *See* 45 CFR 164.306(a)(2).

[67] *See* 45 CFR 164.306(a)(3).

[68] *See* 45 CFR 164.306(a)(4).

[69] *See* sec. 262(a) of Public Law 104–191, 110 Stat. 2025 (Aug. 21, 1996), adding sec. 1173(d) (codified at 42 U.S.C. 1320d–2(d)).

[70] 63 FR 43242 (Aug. 12, 1998).

[71] *Id.* at 43244.

[72] *Id.* at 43244, 43249, 43260–61.

[73] *Id.* at 43249.

[74] *See* 68 FR 8334, 8335 (Feb. 20, 2003).

[75] *Id.; see also* 63 FR 43242, 43249 (Aug. 12, 1998).

[76] 63 FR 43242, 43250 (Aug. 12, 1998).

[77] *Id.*

[78] *Id.* at 43249–50.

[79] *Id.* at 43250.

[80] 45 CFR parts 160 and subparts A and C of 45 CFR part 164; 68 FR 8334 (Feb. 20, 2003).

[81] 68 FR 8334, 8335, 8371–72 (Feb. 20, 2003).

[82] *Id.*

[83] *Id.*

[84] *Id.* at 8335.

[85] *Id.*

[86] *Id.* at 8336.

explained, do not allow organizations to make their own rules, only their own technology choices.[87]

We also recognized that entities could minimize risk through their security practices, but likely could never completely eliminate all risk. In the preamble to the 2003 Final Rule, the Department acknowledged that there is no such thing as a totally secure system that carries no risks to security.[88] The Department opined that Congress' intent in the use of the word ''ensure'' in section 1173(d) of the SSA was to set an exceptionally high goal for the security of ePHI. However, we also recognized that Congress anticipated that some trade-offs would be necessary, and that ''ensuring'' protection did not mean doing so without any regard to the cost.[89] As such, the Department explained that we expected a covered entity to protect that information to the best of its ability.[90] Thus, a covered entity would be expected to balance the identifiable risks to and vulnerabilities of ePHI with the cost of various protective measures, while also taking into consideration the size, complexity, and capabilities of the covered entity.[91]

In the 2003 Final Rule, the Department introduced the concept of ''addressable'' implementation specifications, which it distinguished from ''required'' implementation specifications. The goal was to provide covered entities with even more flexibility.[92] While none of the implementation specifications were optional, designating some of the implementation specifications as addressable provided each covered entity with the ability to determine whether certain implementation specifications were reasonable and appropriate safeguards for that entity, based on its risk analysis, risk mitigation strategy, previously implemented security measures, and the cost of implementation.[93]

3. 2009 Delegation of Authority

On October 7, 2003, the Secretary delegated authority for administering and enforcing the Security Rule to the Administrator of the Centers for Medicare & Medicaid Services (CMS).[94] The Secretary issued a notice on August 4, 2009, superseding the previous delegation and replacing it with a delegation authority to the Director of OCR effective July 27, 2009.[95]

4. 2013 Omnibus Rulemaking

Following the enactment of the HITECH Act, the Department issued an NPRM, entitled ''Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health [HITECH] Act'' (''2010 Proposed Rule''),[96] to propose implementation of certain HITECH Act requirements. In the 2010 Proposed Rule, the Department noted that it had not amended the Security Rule since 2003.[97] We further explained that information gleaned from contact with the public since that time, OCR's enforcement experience, and technical corrections needed to eliminate ambiguity provided the impetus for the Department's actions to propose certain regulatory changes beyond those required by the HITECH Act.[98]

In 2013, the Department issued the final rule ''Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health [HITECH] Act and the Genetic Information Nondiscrimination Act, and Other Modifications to the HIPAA Rules'' (''2013 Omnibus Rule''),[99] which implemented applicable provisions of the HITECH Act to strengthen security protections for individuals' health information maintained in EHRs.

For example, the Department modified the Security Rule to implement the HITECH Act's provisions that extended direct liability for compliance with the Security Rule to business associates.[100] We explained that before the enactment of the HITECH Act, the Security Rule did not directly apply to business associates of covered entities. The HITECH Act extended the application of the Security Rule's administrative, physical, and technical safeguards requirements, as well as the rule's policies and procedures and documentation requirements, to business associates in the same manner as the requirements apply to covered entities, making those business associates civilly and criminally liable for violations of the Security Rule.[101] The Department noted that the Security Rule requires a covered entity to establish business associate agreements that obligate business associates to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that they create, receive, maintain, or transmit on behalf of the covered entity.[102] Accordingly, we reasoned that business associates and subcontractors should already have security practices in place that comply with the Security Rule, or require only modest improvement to come into compliance with the Security Rule requirements.[103] Like the 2003 Final Rule,[104] the 2013 Omnibus Rule highlighted that the Security Rule was designed to be technology neutral and scalable and reiterated that regulated entities have the flexibility to choose security measures appropriate for their size, resources, and the nature of the security risks they face.[105] Accordingly, regulated entities have the flexibility to choose appropriate security measures considering their size, capabilities, the costs of the specific security measures, and the operational impact, enabling them to reasonably implement the standards of the Security Rule.

The Department also adopted technical revisions to 45 CFR 164.306(e) to clarify that regulated entities must review and modify security measures as needed to ensure reasonable and appropriate protection of ePHI, and update documentation of security measures accordingly.[106]

Finally, because the HITECH Act made business associates directly liable for compliance with the Security Rule, the 2013 Omnibus Rule modified the Security Rule to clarify that a covered entity is not required to obtain satisfactory assurance from a business associate that is a subcontractor that the subcontractor will appropriately safeguard its ePHI. Rather, the business

[87] *Id.* at 8343.

[88] *Id.* at 8346.

[89] *Id.*

[90] *Id.*

[91] *Id.*

[92] *Id.*

[93] *Id.* at 8336.

[94] ''Statement of Organization, Functions, and Delegations of Authority,'' Centers for Medicare & Medicaid Services, 68 FR 60694 (Oct. 23, 2003).

[95] ''Office for Civil Rights; Delegation of Authority,'' U.S. Department of Health and Human Services, 74 FR 38630 (Aug. 4, 2009); *see also* ''Statement of Organization, Functions, and Delegations of Authority,'' Centers for Medicare & Medicaid Services, 74 FR 38663 (Aug. 4, 2009).

[96] 75 FR 40868 (July 14, 2010).

[97] *Id.* at 40871.

[98] *Id.*

[99] 78 FR 5565 (Jan. 25, 2013). In addition to finalizing requirements of the HITECH Act that were proposed in the NPRM, the Department adopted modifications to the Enforcement Rule not previously adopted in an earlier interim final rule, 74 FR 56123 (Oct. 30, 2009), and to the Breach Notification Rule not previously adopted in an interim final rule, 74 FR 42739 (Aug. 24, 2009). The Department also finalized previously proposed Privacy Rule modifications as required by the Genetic Information Nondiscrimination Act of 2008, 74 FR 51698 (Oct. 7, 2009).

[100] 78 FR 5565, 5589 (Jan. 25, 2013).

[101] Sec. 13401 of Public Law 111–5, 123 Stat. 260 (Feb. 17, 2009) (codified at 42 U.S.C. 17931).

[102] 78 FR 5565, 5590 (Jan. 25, 2013); *see also* 45 CFR 164.314(a).

[103] 78 FR 5565, 5589 (Jan. 25, 2013).

[104] 68 FR 8334, 8341 (Feb. 20, 2003).

[105] 78 FR 5565, 5589 (Jan. 25, 2013).

[106] *Id.* at 5590.

associate of the covered entity must obtain the required satisfactory assurances from the subcontractor to protect the security of ePHI.[107]

III. Justification for This Proposed Rulemaking

HIPAA and the HIPAA Rules promote access to high-quality and effective health care by establishing standards for the security of ePHI. The standards, when implemented appropriately by regulated entities, protect the confidentiality, integrity, and availability of individuals' health information. Such protections promote the electronic transmission of PHI through a national health information system. To ensure access to high-quality health care services, regulated entities must assure their customers (*e.g.,* individuals, health care providers, and health plans) of the security of the sensitive and confidential health information the regulated entities electronically create, receive, maintain, or transmit.

As discussed above, the Security Rule carefully balances the benefits of safeguarding against security risks with the burdens of implementing protective measures by permitting regulated entities to consider several factors, including costs and available technology for preventing and mitigating security risks,[108] when determining which security measures are reasonable and appropriate for protecting the security of individuals' ePHI.[109]

For example, the Security Rule requires that a regulated entity implement policies and procedures to limit physical access to its electronic information systems and the facilities in which they are housed, while ensuring that users who are authorized to access such information systems and facilities are permitted to do so.[110] The implementation specifications associated with this standard only address the need for operationalized policies and procedures related to specific aspects of physical security.[111] They do not dictate the specifics of such policies and procedures because we recognize that the nature of the physical safeguards should depend on the type of regulated entity, its size, its level of access to ePHI, and a number of other factors.

Since the Security Rule's promulgation in 2003, the environment in which health care is provided and in which regulated entities operate has changed significantly, including transformative changes in how regulated entities create, receive, maintain, and transmit ePHI. For example, as of 2021, almost 80 percent of physician offices and 96 percent of hospitals had adopted certified EHRs.[112] The use of health IT, including EHRs (certified or otherwise), has led to enormous advancements in the fields of medicine and public health, not only improving outcomes for individuals, but also assisting in addressing the social, economic, and environmental factors that affect health on an individual and community level.[113] And the electronic exchange of health information, spurred by HIPAA, the HITECH Act, and the 21st Century Cures Act (''Cures Act''),[114] has enabled regulated entities and others to more quickly and efficiently share individuals' health information, increasing the quality and efficiency of health care, increasing patient engagement, and reducing administrative burden.[115] However, the widespread use of health IT systems makes it even more critical for regulated entities, regardless of their size or location, to fully assess the risks and vulnerabilities to ePHI and their information systems and implement strong security measures to address those risks and vulnerabilities.

Experts repeatedly have expressed concern regarding the state of cybersecurity in the health care industry.[116] For example, in a 2017 report to Congress, experts convened by the Department pronounced, ''Now more than ever, all health care delivery organizations [. . .] have a greater responsibility to secure their systems, medical devices, and patient data.'' [117] This responsibility has only increased as the delivery of health care and the exchange of PHI have increasingly shifted to cyberspace.

Despite advancements in technology, including health IT, the core requirements of the Security Rule remain relevant and applicable today. In fact, they serve as a foundation for more recently promulgated cybersecurity guidelines, best practices, processes, and procedures. Security management, regular monitoring and review of information system activity, information access management, security awareness and training, contingency planning, encryption, and authentication all continue to be represented in the most well-known cybersecurity frameworks, including the NIST's Cybersecurity Framework,[118] the HHS 405(d) Program's ''Health Industry Cybersecurity Practices: Managing

[107] *Id.* (citing 45 CFR 164.308(b)).

[108] As technology has evolved and cybercriminals have become more sophisticated, protective measures, including technology, have been developed to prevent and mitigate such risks. For example, certain health IT may be certified through the ONC Health IT Certification Program as meeting certain criteria that address the security of information created, received, maintained, or transmitted by that health IT. *See* 45 CFR 170.550(h).

[109] 45 CFR 164.306(b).

[110] 45 CFR 164.310(a)(1).

[111] 45 CFR 164.310(a)(2).

[112] ''National Trends in Hospital and Physician Adoption of Electronic Health Records,'' The Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, *https://www.healthit.gov/data/quickstats/national-trends-hospital-and-physician-adoption-electronic-health-records.*

[113] *See* ''2020–2025 Federal Health IT Strategic Plan,'' The Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, p. 6 (Oct. 2020), *https://www.healthit.gov/sites/default/files/page/2020-10/Federal%20Health%20IT%20Strategic%20Plan_2020_2025.pdf.*

[114] Among other things, the Cures Act provided ONC, in collaboration with NIST and other relevant agencies within the Department, with the authority to convene public-private and public-public partnerships to build consensus and develop or support a trusted exchange framework, including a common agreement among health information networks nationally. The purpose of this work is to ensure full network-to-network exchange of health information. Sec. 4003(b) of Public Law 114–255, 130 Stat. 1165 (Dec. 13, 2016) (codified at 42 U.S.C. 300jj–11(c)). The Cures Act also provides penalties for any developer of certified health IT, health information exchange or network, and appropriate disincentives for any health care provider, determined by the Inspector General to have committed information blocking. Sec. 4004(b)(2) of Public Law 114–255, 130 Stat. 1165 (Dec. 13, 2016) (codified at 42 U.S.C. 300jj–52).

[115] *See* ''Frequently Asked Question: Health Information Exchange: The Benefits,'' The Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, *https://www.healthit.gov/faq/why-health-information-exchange-important.*

[116] *See* Genevieve P. Kanter, et al., ''Beyond Security Patches—Fundamental Incentive Problems in Health Care Cybersecurity,'' JAMA Health Forum, Volume 2, Issue 10, p. e212969 (Oct. 8, 2021), *https://jamanetwork.com/journals/jama-health-forum/fullarticle/2784981;* Chon Abraham, et al., ''Muddling through cybersecurity: Insights from the U.S. healthcare industry,'' Business Horizons, Volume 62, Issue 4, p. 539–548, p. 539 (July-Aug. 2019), *https://www.sciencedirect.com/science/article/abs/pii/S0007681319300436;* Eric Perakslis, ''Responding to the Escalating Cybersecurity Threat to Health Care,'' The New England Journal of Medicine, Volume 387, Issue 9 (Sept. 1, 2022), *https://www.nejm.org/doi/abs/10.1056/NEJMp2205144;* Anthony James Cartwright, ''The elephant in the room: cybersecurity in healthcare,'' Journal of Clinical Monitoring and Computing, Volume 37, Issue 5, p. 1123–1132 (Apr. 24, 2023), *https://link.springer.com/article/10.1007/s10877-023-01013-5.*

[117] ''Report on Improving Cybersecurity In The Health Care Industry,'' Health Care Industry Cybersecurity Task Force, p. 1 (June 2017), *https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf.*

[118] ''The NIST Cybersecurity Framework (CSF) 2.0,'' *supra* note 15.

Threats and Protecting Patients,'' [119] and the Department's CPGs.[120]

While these concepts remain highly relevant and applicable, the Department has concerns regarding the sufficiency of the security measures implemented by regulated entities. OCR's experience investigating allegations of Security Rule violations, reports received by OCR of breaches of unsecured PHI, and the results of the audits conducted by OCR in 2016–2017 demonstrate that regulated entities are not consistently complying with the Security Rule's requirements.[121] Additionally, the Department is concerned about the extent to which regulated entities have updated their security measures to adjust to the changes in the health care environment and their operations, including new and emerging threats to the confidentiality, integrity, and availability of ePHI.

And the Department is not alone in its concerns. NCVHS serves as the Department's advisory body for HIPAA.[122] Given the increase in cybersecurity incidents affecting the health care sector, NCVHS held a series of public hearings on cybersecurity to better understand how to protect ePHI and individuals. In response to those hearings, NCVHS submitted several recommendations to the Department regarding the importance of strengthening the Security Rule.[123] As discussed above, HIPAA requires the Secretary to rely on NCVHS' recommendations [124] with respect to standards promulgated under the statute.

Given the importance of strong security measures, the changed environment and operations for health care, uncertainty expressed by regulated entities regarding their compliance obligations, deficiencies identified by OCR in its investigations of regulated entities, and the recommendations of NCVHS, we believe that it is necessary and appropriate for the Department to propose modifications to clarify and strengthen the Security Rule.

A. Strong Security Standards Are Essential to Protecting the Confidentiality, Integrity, and Availability of ePHI and Ensuring Quality and Efficiency in the Health Care System

A primary purpose of HIPAA's Administrative Simplification provisions [125] is to, among other things, ''improve [. . .] the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of uniform standards and requirements for the electronic transmission of certain health information.'' [126] As Congress recognized when it enacted HIPAA, protecting the security of ePHI is essential for accomplishing this goal. Members of Congress acknowledged at that time that the provisions of HIPAA would create electronic databases of PHI, enabling the PHI to be transmitted electronically with both the benefits and risks that accompany such electronic transactions.[127] Congressional statements leading up to HIPAA's enactment demonstrate Congress' recognition of the potential risks of the shift from paper recordkeeping to electronic: ''We need to be very careful about how safe and secure that information is from prying eyes. Some of it may be extremely sensitive and could be used in a malicious or discriminatory manner.'' [128] Accordingly, HIPAA required the establishment of strict security standards for health information.

As discussed above, the Security Rule, as amended by the HITECH Act, specifically requires regulated entities to maintain reasonable and appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI; to protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI and unauthorized uses or disclosures of ePHI; and ensure compliance with the Administrative Simplification provisions by officers and workforce members of regulated entities.[129]

It is reasonable to anticipate that regulated entities will need to protect ePHI against cyberattacks and unauthorized uses and disclosures of ePHI by their workforce members. Experts estimate the costs to the U.S. from cyberattacks on health care facilities to be significant.[130] According to one study, health care data breach costs to affected organizations have increased by more than 50 percent since 2020, making health care data breaches more expensive than data breaches in any other sector, at an average cost of almost $10.1 million per breach.[131] Yet these costs, though sizeable, do not fully take into account the practical implications of poor or ineffective cybersecurity protocols. A failure to implement adequate security measures may lead to: financial loss; reputational harm for affected individuals and affected regulated entities; privacy loss; and safety concerns.[132] Additionally, breaches of unsecured PHI may lead to identity theft, fraud, stock manipulation, and competitive disadvantage.[133] According to a study funded by the Institute for Critical Infrastructure Technology, victims of medical identity theft incur on average costs of $13,500 to recover from that theft.[134] Unlike financial information, much of an individual's PHI is

[119] ''Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients,'' *supra* note 16.

[120] ''Cybersecurity Performance Goals,'' *supra* note 18.

[121] *See* ''2016–2017 HIPAA Audits Industry Report,'' Office for Civil Rights, U.S. Department of Health and Human Services (Dec. 2020), *https://www.hhs.gov/sites/default/files/hipaa-audits-industry-report.pdf.*

[122] *See* sec. 262 of Public Law 104–191, 110 Stat. 2023 (Aug. 21, 1996) (codified at 42 U.S.C. 1320d–1(f)), added sec. 1172(f) of the SSA; *see also* ''About NCVHS,'' National Committee on Vital and Health Statistics, *www.ncvhs.hhs.gov.*

[123] *See* Letter from NCVHS Chair Jacki Monson to HHS Secretary Xavier Becerra (May 10, 2022), *https://ncvhs.hhs.gov/wp-content/uploads/2022/05/NCVHS-Recommendations-to-Strengthen-Cybersecurity-in-HC-05-10-2022-508.pdf; see also* Letter from NCVHS Chair Jacki Monson to HHS Secretary Xavier Becerra (Nov. 29, 2023), *https://ncvhs.hhs.gov/wp-content/uploads/2024/01/Letter-to-the-Secretary-Recommendations-to-Strengthen-the-HIPAA-Security-Rule_508.pdf.*

[124] 42 U.S.C. 1320d–1(f).

[125] Subtitle F of title II of HIPAA, Public Law 104–191, 110 Stat. 1936 (Aug. 21, 1996).

[126] Sec. 261 of Public Law 104–191, 110 Stat. 2021 (Aug. 21, 1996), as amended by sec. 1104(a) of Public Law 111–148, 124 Stat. 146 (Mar. 23, 2010) (codified at 42 U.S.C. 1320d note).

[127] *See* statement of Sen. Simon, *supra* note 34; *see also* 155 Cong. Rec. H1562 (statement of Rep. Markey) (stating that ARRA includes provisions for health IT with built-in privacy and security); Implementation of the Health Information Technology for Economic and Clinical Health (HITECH) Act: Hearing Before the House Committee on Energy and Commerce Subcommittee on Health, 111th Cong. 11–12 (2010) (statement of Rep. Schakowsky) (explaining that the HITECH Act strengthened Federal privacy and security laws to protect personal identifying information from misuse to ensure that individuals would be willing to use electronic records).

[128] Statement of Sen. Simon, *supra* note 34.

[129] *See* section 1173(d)(2) of HIPAA (codified at 42 U.S.C. 1320d–2(d)(2)) and section 13401 of ARRA (codified at 42 U.S.C. 17931(a)) and 45 CFR 164.306.

[130] *See* Hadi Ghayoomi, et al., ''Assessing resilience of hospitals to cyberattack,'' Digital Health, p. 2 (2021), *https://doi.org/10.1177/20552076211059366;* ''Beyond Security Patches–Fundamental Incentive Problems in Health Care Cybersecurity,'' *supra* note 116; Jessica Brewer, et al., ''An Insight into the Current Security Posture of Healthcare IT: A National Security Concern,'' The Institute for Critical Infrastructure Technology, p. 3 (2019), *https://www.icitech.org/post/an-insight-into-the-current-security-posture-of-healthcare-it-a-national-security-concern.*

[131] ''Cost of a Data Breach Report 2023,'' IBM, p. 13 (2023) (explaining that the average cost of a health care data breach was $7.13 million in 2020), *https://www.ibm.com/reports/data-breach.*

[132] ''Report on Improving Cybersecurity In The Health Care Industry,'' *supra* note 117, p. 14–15.

[133] *Id.*

[134] ''An Insight into the Current Security Posture of Healthcare IT: A National Security Concern,'' *supra* note 130, p. 3.

immutable. For example, an individual's date and location of birth and their health history will not change, even if their address might. In contrast, an individual's passwords, bank account numbers, and other financial information can all be changed. Thus, PHI can continue to be exploited throughout an individual's lifetime, making PHI likely to be far more valuable than an individual's credit card information.[135]

On the surface, the harms that result from a breach of ePHI or a cyberattack on a regulated entity's electronic information systems, as discussed above, are not significantly different than those that would result from a breach of information in another sector. However, the reality is, as discussed above, that the implications of such harms are far greater in the health care sector because of their potential to adversely affect an individual's health or quality of life, or even to cost an individual their life.[136] As stated by the Health Care Industry Cybersecurity Task Force in its 2017 report on the state of cybersecurity in health care: ''The health care system cannot deliver effective and safe care without deeper digital connectivity. If the health care system is connected, but insecure, this connectivity could betray patient safety, subjecting them to unnecessary risk and forcing them to pay unaffordable personal costs.'' [137] In the event of a cybersecurity incident, patients' health, including their lives, may be at risk where such incident creates impediments to the provision of health care, such as interference with the operations of a critical medical device, or to the administrative or clinical operations of a regulated entity, such as preventing the scheduling of appointments or viewing of an individual's health history.[138]

According to a Cybersecurity & Infrastructure Security Agency (CISA) statistical analysis of the effects of a hypothetical cyberattack on a model hospital, a hospital's relative performance will suffer amidst a cyberattack.[139] The analysis found that the hypothetical cyberattack would lead to hospital strain from inaccessible patient schedules and records, disrupted communication, and delays in processing and communicating test results in time to effectively treat individuals.[140] While the analysis did not find any deaths directly attributable to the hypothetical attack, it is logical to conclude that deaths—or at least worsened outcomes—are a significant risk where there are disruptions in communications, as well as delays in processing and communicating test results, especially for emergent or acute medical cases. For example, an inability to access an individual's pharmacy records could affect the ability of a pharmacist to identify known interactions between newly prescribed medications and an existing medication list, potentially leading to an individual's injury or death. Other studies have similarly found that cyberattacks can have a substantial effect on access to health care, and potentially mortality.[141] In fact, a more recent study found that cyberattacks had disproportionately negative effects on in-hospital mortality rates for Black patients who were already admitted to the hospital at the time of the cyberattack.[142] A recent survey found that 92 percent of surveyed health care organizations had experienced a cyberattack in the past year [143] and almost three-quarters of the respondents who had experienced a cyberattack reported negative effects on patient care, including delays in tests or procedures, longer stays, and increased mortality rates complications from medical procedures, and patient transfers or diversions to other facilities.[144] A recent letter from NCVHS referenced anecdotal accounts of patient deaths that have been attributed to ransomware attacks.[145] For example, in 2019, a ransomware attack may have contributed to a baby's death at an Alabama hospital. A change in the baby's fetal heart rate went unnoticed because the large digital display that normally would have displayed the information was affected by the attack. The baby, born with her umbilical cord wrapped around her neck, suffered severe brain damage and died nine months later.[146]

Cyberattacks can divert both human and machine resources, leading to process slowdowns, cancelled procedures, delayed hospital or unit lockdowns and transfers, increases in wait times for individuals, both increases and decreases in staff utilization, and a decrease in a health care provider's capacity.[147] A 2020 cyberattack on a large integrated academic health system, attributed to malicious software embedded in an email attachment opened by an employee on their laptop, affected more than 5,000 end-user devices across 1,300 servers and led to revenue losses of more than $63 million.[148] Though the health care provider's EHR was not infected, it elected to shut the EHR down proactively. Ultimately, the covered entity ''experienced 39 days of downtime in outpatient imaging.'' [149]

In another example, a ransomware attack on an academic level 1 trauma center caused it to go without access to its EHR for 25 days,[150] and the attack affected 5,000 computers and destroyed the trauma center's electronic information systems that contained ePHI. The hospital lost access to its EHR, internet, and intranet, which also ''removed functionality of hospital phones, [EHR] integrated office and surgical scheduling, access to digitized radiology studies, and network account access through local and remote computers.'' [151]

These serious incidents and resulting effects demonstrate the importance of planning and preparing for a potential

---

[135] *See, e.g., Caleb J. Kumar,* ''*New Dangers in the New World: Cyber Attacks in the Healthcare Industry,*'' *Intersect, Volume 10, No. 3, p. 3 (2017).*

[136] ''An Insight into the Current Security Posture of Healthcare IT: A National Security Concern,'' *supra* note 130, p. 3.

[137] ''Report on Improving Cybersecurity In The Health Care Industry,'' *supra* note 117, p. 2.

[138] *Id.* at 18.

[139] ''CISA INSIGHTS: Provide Medical Care Is In Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm,'' Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security, p. 12–15 (Sept. 2021), *https://www.cisa.gov/sites/default/files/publications/CISA_Insight_Provide_Medical_Care_Sep2021.pdf.*

[140] *Id.*

[141] *See* ''Assessing resilience of hospitals to cyberattack,'' *supra* note 130; Claire C. McGlave, et al., ''Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients,'' SSRN (Oct. 4, 2023), *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4579292.*

[142] ''Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients,'' *supra* note 141, p. 14.

[143] ''The 2024 Study on Cyber Insecurity In Healthcare: The Cost and Impact on Patient Safety and Care,'' Ponemon Institute, p. 3 (2024) (The report, sponsored by Proofpoint, Inc., included survey responses from 648 IT and IT security practitioners at U.S.-based health care organizations.).

[144] *Id.* at p. 5.

[145] *See* Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, p. 1 (citing several media reports that attributed patient deaths to cybersecurity attacks).

[146] *Id.* (citing Joseph Marks, ''Ransomware attack might have caused another death,'' The Washington Post (Oct. 1, 2021), *https://www.washingtonpost.com/politics/2021/10/01/ransomware-attack-might-have-caused-another-death/*).

[147] ''Assessing resilience of hospitals to cyberattack,'' *supra* note 130, p. 2.

[148] Kerri Reeves, ''Cyberattacks: Not a Matter of If, but When,'' Radiology Matters (Mar./Apr. 2024), *https://www.proquest.com/scholarly-journals/cyberattacks-not-matter-if-when/docview/2957757956/se-2?accountid=12786.*

[149] *Id.*

[150] Mitchell Tarka, et al., ''The crippling effects of a cyberattack at an academic level 1 trauma center: An orthopedic perspective,'' Injury, p. 1095–1101 (2023), *https://pubmed.ncbi.nlm.nih.gov/36801172/.*

[151] *Id.*

cyberattack or other event that adversely affects a regulated entity's information systems. While such planning and preparation may not prevent all cyberattacks, it can reduce the number of successful incidents and mitigate their effects. In fact, studies have suggested that such preparation may allow for at least close to real-time recovery.[152]

The effects of a cyberattack are not limited to the regulated entity that experiences it and the individuals whose ePHI is compromised. Surveys conducted by various organizations representing health care providers indicate that an overwhelming majority of health care providers in the U.S. were affected by a ransomware attack on a large health care clearinghouse.[153] A study published in 2023 examined the effects on the of a cyberattack at a neighboring, unaffiliated hospital on a large academic medical center.[154] The study found that the academic medical center experienced, among other things, significant increases in the number of patients admitted, ambulance arrivals, waiting room times, and patients leaving without being seen. The study's authors concluded that their findings suggested ''that health care cyberattacks such as ransomware are associated with greater disruptions to regional hospitals and should be treated as disasters, necessitating coordinated planning and response efforts.'' [155] Thus, implementing reasonable and appropriate security measures better protects not only the regulated entity and its ePHI, but other regulated entities with whom it interacts, and may reduce the effects of cyberattacks and other security incidents that adversely affect the confidentiality, integrity, or availability of ePHI.

As discussed above, several industry organizations have published and maintained compilations of voluntary standards, guidelines, best practices, methodologies, procedures, and processes for protecting the security of sensitive and confidential information, including PHI. Additionally, certain Federal health programs now either require or recommend the adoption of specific criteria that are intended to protect the confidentiality, integrity, and availability of ePHI. For example, the Health IT Certification Program maintained by the Assistant Secretary for Technology Policy and Office of the National Coordinator for Health Information Technology (ASTP/ONC) [156] sets minimum requirements for certified health IT, including criteria that pertain to cybersecurity.[157] These criteria are included in the Health IT Certification Program's Health IT Privacy and Security Framework,[158] which identifies *when technical capabilities to support* the privacy and security of electronic health information [159] must be included in certified health IT products. Additionally, health care providers that participate in certain Federal health programs must use health IT certified to these requirements.[160] Regulated entities also may want to consider adoption of certified health IT because it could contribute to compliance with the Security Rule. We will continue to work across the Department to ensure the adoption of consistent requirements for Federal programs that support the secure electronic exchange of health information to the extent that such consistency is appropriate. Throughout this preamble, we provide examples of how a regulated entity's participation in other Federal programs that require the use of health IT certified through the ONC Health IT Certification Program, or adoption of other Federal recommendations, such as the HHS CPGs, might support their compliance with the proposals in this NPRM.

Additionally, as discussed above, several organizations have published and maintained compilations of voluntary standards, guidelines, best practices, methodologies, procedures, and processes for protecting the security of sensitive and confidential information, including PHI. These compilations and the State regulations discussed above range from granular [161] to high-level [162] and from health care-specific [163] to industry agnostic.[164] Despite these differences, these compilations and regulations have a great deal in common with each other—and with the Security Rule, its longevity notwithstanding. In fact, the foundational elements of the Security Rule, promulgated more than 20 years ago, can still be found in cybersecurity compilations published today. They generally either require or recommend administrative, physical, and technical safeguards to identify and mitigate risks and vulnerabilities, implement authentication and access controls, conduct security awareness and training for information system users, and plan for contingencies and incident response.[165] Additionally, these compilations all require or recommend the designation of a specific individual who is accountable for implementing the requirements or recommendations. And, importantly, they all ultimately address how to maintain the

[152] ''Assessing resilience of hospitals to cyberattack,'' *supra* note 130, p. 13.

[153] *See* Paige Minemyer, ''AMA: 80% of docs have lost revenue amid disruptions from Change Healthcare cyberattack,'' Fierce Healthcare (Apr. 10, 2024), *https://www.fiercehealthcare.com/practices/ama-80-docs-have-lost-revenue-amid-disruptions-change-healthcare-cyberattack;* ''AHA survey: Change Healthcare cyberattack having significant disruptions on patient care, hospitals' finances'' (Mar. 15, 2024), *https://www.aha.org/news/news/2024-03-15-aha-survey-change-healthcare-cyberattack-having-significant-disruptions-patient-care-hospitals-finances; see also* Sean Lyngaas, '' 'We're hemorrhaging money': US health clinics try to stay open after unprecedented cyberattack,'' CNN (Mar. 9, 2024), *https://www.cnn.com/2024/03/09/tech/medical-supply-chain-cybersecurity/index.html.*

[154] Christian Dameff, et al., ''Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the U.S.,'' JAMA Network Open (May 8, 2023), *https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2804585.*

[155] *Id.*

[156] On July 29, 2024, the Department announced that the Office of the National Coordinator for Health Information Technology was being renamed the Assistant Secretary for Technology Policy and Office of the National Coordinator for Health Information Technology. In this NPRM, we continue to use ONC for publications cited that predate the renaming of that office. 89 FR 60903 (July 29, 2024).

[157] *See, e.g.,* 45 CFR 170.315(d)(6), (7), (12), and (13). For more information on the ONC Health IT Certification Program, visit *https://www.healthit.gov/topic/certification-ehrs/certification-health-it.*

[158] The ONC Health IT Certification Program specifies at 45 CFR 170.550(h) the privacy and security certification framework for Health IT Modules. Section 170.550(h) identifies a mandatory minimum set of the certification criteria that ONC-Authorized Certification Bodies (ONC ACBs) must ensure are also included as part of specific Health IT Modules that are presented for certification. *See* ''Certification Companion Guide Privacy and Security,'' The Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (May 7, 2024), *https://www.healthit.gov/sites/default/files/2015Ed_CCG_Privacy_and_Security.pdf.*

[159] *See* 45 CFR 171.102 (definition of ''Electronic health information'').

[160] *See, e.g.,* Medicare Promoting Interoperability Program, 42 CFR 495.24 (eligible hospitals and critical access hospitals must use certified electronic health record technology (CEHRT), with limited exceptions, to comply with the program's meaningful use requirements); Merit-based Incentive Payment System (MIPS) Promoting Interoperability performance category, 42 CFR 414.1375 (requiring MIPS eligible clinicians to use CEHRT, as defined in 42 CFR 414.1305, to comply with reporting requirements for the Promoting Interoperability performance category).

[161] *See, e.g.,* ''Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients,'' *supra* note 16.

[162] *See, e.g.,* ''The NIST Cybersecurity Framework (CSF) 2.0,'' *supra* note 15.

[163] *See, e.g.,* ''Cybersecurity Performance Goals,'' *supra* note 18.

[164] *See, e.g.,* ''Cross-Sector Cybersecurity Performance Goals,'' Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security (Mar. 2023), *https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf.*

[165] *See generally* 45 CFR 164.308(a); ''The NIST Cybersecurity Framework (CSF) 2.0,'' *supra* note 15; ''Cybersecurity Performance Goals,'' *supra* note 18.

confidentiality, integrity, and availability of sensitive and confidential information, including ePHI.

A major distinguishing factor between the content of the Security Rule and these compilations and regulations is the Security Rule's scope. The compilations and regulations are designed to protect various types of data and information systems broadly. In comparison, a defining quality of the Security Rule's requirements is that they focus specifically on the protection of ePHI and the information systems that create, receive, maintain, or transmit ePHI. Thus, while the foundational elements of various cybersecurity compilations and State regulations and the Security Rule may be the same, the Security Rule alone addresses the application of those elements to ePHI and all of the components of information systems that create, receive, maintain, or transmit ePHI. Thus, while the standards of the Security Rule generally align with those of other cybersecurity standards, frameworks, best practices, guidelines, processes, and procedures, the specific implementation specifications of the Security Rule reflect the particular sensitivities of the health care industry, particularly small and rural health care providers, in a way that is necessary to ultimately improve the efficiency and effectiveness of the health care system and avoid imposing unreasonable compliance burdens on regulated entities.

B. The Health Care Environment Has Changed Since the Security Rule Was Last Revised and Will Continue To Evolve

The health care sector has undergone a dramatic transformation over the last 24 years, and particularly in the past 10 years, spurred at least in part by the Department's implementation of HIPAA, the HITECH Act, and the Cures Act. The industry has shifted from one that generally relied upon a system of paper-based recordkeeping and siloed devices to one that depends on interconnected information systems to maintain and exchange patient records, conduct research, run health care provider facility management systems, and provide patient care.[166] This shift is largely the result of HIPAA's emphasis on the development and use of standards and the EHR incentive funds made available under the HITECH Act for health care providers.[167] Data from ASTP/ONC offer clear and convincing evidence of this shift. In 2008, before the enactment of the HITECH Act, less than 10 percent of non-Federal acute hospitals had implemented what was referred to at the time as a ''Basic EHR'' (*i.e.,* an electronic health record).[168] By 2015, six years after the enactment of the HITECH Act, almost 84 percent had adopted a Basic EHR while 96 percent had adopted a certified EHR.[169] The transformation was further enabled by the Cures Act, which encouraged the development of a trusted exchange framework for the nationwide exchange of health information and provided penalties for health care providers, health information exchanges and networks, and developers of certified health IT that engage in information blocking.[170] In 2014, 41 percent of such hospitals routinely had electronic access to clinical information from outside providers or sources when treating a patient.[171] By 2023, 70 percent of non-Federal acute care hospitals engaged in all domains of interoperable exchange routinely or sometimes, a significant leap forward.[172] In 2017, only 38 percent of hospitals enabled patients to access their health information using an application and in 2018, 57 percent enabled patient access to their clinical notes in their patient portal; by 2021, 70 percent of hospitals enabled patients to access their health information using an application and 82 percent enabled patients to view their clinical notes in their patient portal.[173] And just a year later, the percentage of hospitals that supported patient access through applications increased to 86 percent.[174] Based on this data, it is clear that HIPAA, coupled with the HITECH Act and the Cures Act, has successfully encouraged the development of a nationwide electronic health information system.

Not only is PHI increasingly maintained and transmitted electronically, but treatment is also increasingly provided electronically. The coronavirus disease 2019 (COVID–19) pandemic led to a dramatic increase in the use of telemedicine.[175] According

[166] Derrick Tin, et al., ''Cyberthreats: A primer for health care professionals,'' The American Journal of Emergency Medicine, p. 182–183 (Apr. 2023), *https://doi.org/10.1016/j.ajem.2023.04.001.*

[167] *See* Public Law 104–191, 110 Stat. 2021 (Aug. 21, 1996) (codified at 42 U.S.C. 1320d note); Sec. 4101 of ARRA, Public Law 111–5, 123 Stat. 467 (Feb. 17, 2009), amending sec. 1848 of the SSA (codified at 42 U.S.C. 1395w–4).

[168] JaWanna Henry, et al., ''ONC Data Brief: Adoption of Electronic Health Record Systems among U.S. Non-Federal Acute Care Hospitals: 2008–2015,'' The Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, p. 1 (May 2016), *https://www.healthit.gov/sites/default/files/briefs/2015_hospital_adoption_db_v17.pdf;* A Basic EHR collects information on patient demographics, problem lists, medication lists, and discharge summaries. It also includes computerized provider order entry for medications and enables clinicians to view certain reports. *Id.* at Appendix.

[169] ''ONC Data Brief: Adoption of Electronic Health Record Systems among U.S. Non-Federal Acute Care Hospitals: 2008–2015,'' *supra* note 168, p. 1; When used here, ''certified EHR Technology'' means EHR technology that meets the technological capability, functionality, and security requirements adopted by the Department as certification criteria at 45 CFR part 170.; *see also* ''Certified EHR Technology,'' The Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (Sept. 6, 2013), *https://www.cms.gov/medicare/regulations-guidance/promoting-interoperability-programs/certified-ehr-technology* (''In order to efficiently capture and share patient data, health care providers need certified electronic health record (EHR) technology (CEHRT) that stores data in a structured format. Structured data allows health care providers to easily retrieve and transfer patient information and use the EHR in ways that can aid patient care.'').

[170] *See* sec. 4003(b) and 4004(b)(2) of Public Law 114–255, 130 Stat. 1165 (Dec. 13, 2016) (codified at 42 U.S.C. 300jj–11(c) and 42 U.S.C. 300jj–52).

[171] Dustin Charles, et al., ''ONC Data Brief: Interoperability among U.S. Non-federal Acute Care Hospitals, 2014,'' The Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, p. 1 (Aug. 2015), *https://www.healthit.gov/sites/default/files/briefs/onc_databrief25_interoperabilityv16final_081115.pdf.*

[172] Meghan Hufstader Gabriel, et al., ''ONC Data Brief: Interoperable Exchange of Patient Health Information Among U.S. Hospitals: 2023,'' The Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, p. 1 (May 2024), *https://www.healthit.gov/sites/default/files/2024-05/Interoperable-Exchange-of-Patient-Health-Information-Among-U.S.-Hospitals-2023.pdf.*

[173] Wesley Barker, et al., ''ONC Data Brief: Hospital Capabilities to Enable Patient Electronic Access to Health Information, 2021,'' The Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, p. 2 and 5 (Oct. 2022) (estimates based on non-Federal acute care hospitals and applications configured to meet the application programming interface (API) specifications in the hospital's EHR), *https://www.healthit.gov/sites/default/files/2022-12/hospital_capabilities_to_enable_patient_access_ONC_DB2021-Updated.pdf.*

[174] Catherine Strawley, et al., ''ONC Data Brief: Hospital Use of APIs to Enable Data Sharing Between EHRs and Apps,'' The Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, p. 2 (Sept. 2023) (estimates based on non-Federal acute care hospitals using standards-based APIs to enable patient access), *https://www.healthit.gov/sites/default/files/2023-09/DB68-Hospital%20Use%20of%20APIs%20to%20Enable%20Data%20Sharing_508.pdf.*

[175] *See* ''Determination That A Public Health Emergency Exists Nationwide as the Result of the 2019 Novel Coronavirus,'' Administration for Strategic Preparedness & Response, U.S. Department of Health and Human Services (Jan. 31, 2020), *https://aspr.hhs.gov/legal/PHE/Pages/2019-nCoV.aspx;* ''Renewal of Determination that a Public Health Emergency Exists As a Result of the Continued Consequences of the Coronavirus Disease 2019 (COVID–19) Pandemic,'' Administration for Strategic Preparedness & Response, U.S. Department of Health and Human Services (Feb. 9, 2023), *https://aspr.hhs.gov/legal/PHE/Pages/COVID19-9Feb2023.aspx;* ''Notification of Enforcement Discretion for Telehealth Remote

to ONC data, only 15 percent of office-based physicians used any form of telemedicine in 2018–19. In 2021, telemedicine usage increased to 87 percent.[176] The electronic content generated or transmitted during a telemedicine visit constitutes ePHI, so the increase in telemedicine further increases the amount of PHI that is also ePHI.

It is not only the ePHI maintained in EHRs and other electronic recordkeeping systems that faces security risks. Medical equipment and devices are increasingly connected through one or more networks, which means that any issues affecting the network likely will affect the medical equipment and devices.[177] And some medical equipment and devices rely on off-the-shelf operating systems, such as Windows, Linux, and similar third-party software;[178] thus, the medical equipment and devices can experience the same vulnerabilities as personal computing devices. Generally, the U.S. Food & Drug Administration (FDA) does not need to review software patches or configuration updates for off-the-shelf software before a device manufacturer puts them in place because the FDA views most patches and configuration updates as design changes that can be made without prior discussion.[179]

Cybercriminals may use—or target—technology assets, such as software or medical devices used for treating individuals. For example, in 2021, a cyberattack on cloud-based systems supplied by a particular company compromised the ePHI of more than 200,000 individuals and affected the software for linear accelerators used in radiotherapy, leading to disruptions to cancer treatment.[180] Thus, to protect technology assets used for treatment, the information systems that create, receive, maintain, and transmit ePHI also must be protected. As another example, in 2013, the Mayo Clinic[181] hired a group of ethical hackers[182] to identify vulnerabilities in 40 different medical devices.[183] The hackers were able to gain access to all of the devices, meaning that the devices could all be vulnerable to a cyberattack.[184] Such attacks may create an opening for a subsequent attack on the device itself or on the regulated entity's information systems that create, receive, maintain, or transmit ePHI, compromising those information systems and the ePHI itself.[185] It also may lead, intentionally or not, to a loss of device integrity, which could result in the corruption of the device's functionality or the ePHI on the device.[186] A cyberattack on a medical device may also reduce the ability of the authorized person to use the device (*e.g.,* a denial of service attack, which is a type of cyberattack that overloads the device by flooding the network with traffic).[187] Depending on the device and its use, the result of cyberattacks on a medical device could range from little or no effect to serious injury or death.[188]

According to researchers at Brown University, medical devices are a prime target for cybercriminals. In fact, they believe, ''More than just technically feasible, the widespread takedown of medical devices is an imminent threat.''[189] A 2023 Government Accountability Office report on medical device cybersecurity described the importance of ''robust cybersecurity controls to ensure medical device safety and effectiveness'' because of ''the increasing integration of wireless, internet- and network-connected capabilities, and the electronic exchange of health information.''[190] The FDA has also acknowledged, ''As electronic medical devices become increasingly connected to each other and to other technologies, the ability of connected systems to safely, securely and effectively exchange and use the information becomes critical. [. . .] Cybersecurity concerns rise along with the increasing medical device interoperability.''[191] Accordingly, in 2023, the FDA issued updated guidance for industry and FDA staff on requirements for cybersecurity in medical devices.[192]

And then there are digital health applications. When an application is deployed by a covered entity, an application developer may be a business associate and subject to the Security Rule. An application developer may also meet the HIPAA Rules' definition of ''health care provider''[193] and be a covered entity.[194] But also, individuals are increasingly interested in accessing their ePHI using applications and transmitting information collected by health and wellness applications to

Communications During the COVID–19 Nationwide Public Health Emergency,'' Office for Civil Rights, U.S. Department of Health and Human Services (Jan. 20, 2021), *https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html.*

[176] Yuriy Pylypchuk, et al., ''ONC Data Brief: Use of Telemedicine among Office-Based Physicians, 2021,'' The Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, p. 1 (Mar. 2023), *https://www.healthit.gov/sites/default/files/2023-04/DB65_TelemedicinePhysicians_508.pdf.*

[177] Nduma N. Basil, ''Health Records Database and Inherent Security Concerns: A Review of the Literature,'' Cureus, p. 3 (Oct. 11, 2022) (''The increase in networked medical equipment and devices implies that, if there is a security breach in the form of hacking, then traffic on the network can slow down and interfere with the delivery of healthcare services.''), *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9647912/.*

[178] *Id.*

[179] ''Guidance Document: Information for Healthcare Organizations about FDA's 'Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software,' '' U.S. Food & Drug Administration, U.S. Department of Health and Human Services (Feb. 2005), *https://www.fda.gov/regulatory-information/search-fda-guidance-documents/information-healthcare-organizations-about-fdas-guidance-industry-cybersecurity-networked-medical.*

[180] Elizabeth Gourd, ''Increase in health-care cyberattacks affecting patients with cancer,'' The Lancet, p. 1215 (Sept. 2021), *https://doi.org/10.1016/S1470-2045(21)00451-4.*

[181] *See* Mayo Clinic, *https://www.mayoclinic.org/.*

[182] An ''ethical hacker'' is a cybersecurity researcher who ''use[s] penetration testing techniques to test an organization's cybersecurity and information technology (IT) security.'' *See* Ed Tittel, ''How to Become a White Hat Hacker,'' Business News Daily (June 17, 2024), *https://www.businessnewsdaily.com/10713-white-hat-hacker-career.html.*

[183] *See* Foued Badrouchi, et al., ''Cybersecurity Vulnerabilities in Biomedical Devices: A Hierarchical Layered Framework,'' Internet of Things Use Cases for the Healthcare Industry, p. 157–58 (2020); *see also* Monte Reel, et al., ''It's Way Too Easy to Hack the Hospital,'' Bloomberg Businessweek (Nov. 2015), *https://www.bloomberg.com/features/2015-hospital-hack/.*

[184] *See* ''Cybersecurity Vulnerabilities in Biomedical Devices: A Hierarchical Layered Framework,'' *supra* note 183, p. 157–58.

[185] *See also* ''It's Way Too Easy to Hack the Hospital,'' *supra* note 183; Nicole M. Thomasian, et al., ''Cybersecurity in the internet of Medical Things,'' Health Policy and Technology (Sept. 2021), *https://doi.org/10.1016/j.hlpt.2021.100549.*

[186] ''Cybersecurity in the internet of Medical Things,'' *supra* note 185.

[187] *Id.*

[188] *Id.*

[189] *Id.*

[190] Report to Congressional Committees, ''Medical Device Cybersecurity: Agencies Need to Update Agreement to Ensure Effective Coordination,'' U.S. Government Accountability Office, p. 1 (Dec. 2023), *https://www.gao.gov/assets/d24106683.pdf.*

[191] ''Medical Device Interoperability,'' U.S. Food & Drug Administration, U.S. Department of Health and Human Services, *https://www.fda.gov/medical-devices/digital-health-center-excellence/medical-device-interoperability.*

[192] Guidance for Industry and Food & Drug Administration Staff, ''Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions,'' U.S. Food & Drug Administration, U.S. Department of Health and Human Services (Sept. 27, 2023), *https://www.fda.gov/media/119933/download.*

[193] 45 CFR 160.103 (definition of ''Health care provider'').

[194] Where an application developer meets the HIPAA Rules' definition of health care provider and engages in standard electronic transactions, such as billing an insurance company for its services, it is a covered entity for the purposes of the HIPAA Rules, including the Security Rule. Where an application developer is not regulated under the HIPAA Rules, other Federal laws may apply to the application developer or the application, such as the FTC Act. *See, e.g.,* FTC Act (codified at 15 U.S.C. 41–58).

their health care providers.[195] Such applications may empower individuals to better manage their health and participate in their health care and provide health care providers and researchers with a more holistic view of the individual's health at a particular point in time and over an extended period of time.[196] This technology, while valuable for understanding an individual's overall health, introduces another potential vulnerability to the security of ePHI and the information systems that create, receive, maintain, or transmit it.

EHRs, networked medical devices, and applications are only the beginning. Artificial intelligence (AI) in health care, particularly for diagnosis and treatment, is in the nascent stages of development, but many are eager to test its promise.[197] After all, many experts believe that AI promises opportunities to improve patient care, outcomes, and population health, as well as to reduce costs.[198] The use of AI in health care is increasing and is expected to continue to increase.[199] A 2023 Healthcare Information and Management Systems Society (HIMSS) survey of health care cybersecurity professionals reported that approximately 50 percent of respondents' organizations permitted the use of generative AI technology.[200] And other new technologies are expected shortly, as discussed below. For example, according to reports, quantum computing may be available in the near future, which may have ramifications for data privacy and security.[201] We also know that researchers are exploring methods for storing ePHI in biological material (*e.g.,* DNA).[202]

While the promise of these new technologies is exciting, they come with increased risks and vulnerabilities to ePHI and the information systems that create, receive, maintain, or transmit it. As noted by Executive Order (E.O.) 14110, ''[AI] must be safe and secure. Meeting this goal requires [. . .] addressing AI systems' most pressing security risks—including with respect to biotechnology, cybersecurity, critical infrastructure, and other national security dangers—while navigating AI's opacity and complexity.'' [203] For these reasons, the E.O. required the Secretary of HHS, in consultation with the Secretary of Defense and the Secretary of Veterans Affairs, to establish an HHS AI Task Force to develop a strategic plan that includes policies and frameworks on responsible deployment and use of AI and AI-enabled technologies in the health and human services sector, including the incorporation of safety, privacy, and security standards into the software-development lifecycle for the protection of personally identifiable information, such as measures to address AI-enhanced cybersecurity threats in the health and human services sector.[204] The Department has taken a number of actions to address the use of AI in health care, including establishing an AI Council, appointing a Chief AI Officer,[205] and taking steps to regulate the use of AI in health care.[206] Accordingly, regulated entities must be prepared to identify, mitigate, and remediate such risks and vulnerabilities.

While the health care industry has generally shifted from paper record-keeping and non-interoperable electronic devices to an interconnected electronic health care system, it has led to an increasing vulnerability to breaches of unsecured PHI resulting from unauthorized uses and disclosures and cyberattacks. According to an article published by the American Hospital Association Center for Health Innovation, ''Health care organizations are particularly vulnerable and targeted by cyberattacks because they possess so much information of high monetary and intelligence value to cyber thieves and nation-state actors.'' [207] In fact, ''[. . .] on the dark web, PHI is deemed more

---

[195] *See, e.g.,* Kea Turner, et al., ''Sharing patient-generated data with healthcare providers: findings from a 2019 national survey,'' Journal of the American Medical Informatics Association, p. 371–376 (Nov. 12, 2020), *https://doi.org/10.1093/jamia/ocaa272;* Accenture Federal Services, ''Conceptualizing a Data Infrastructure for the Capture, Use, and Sharing of Patient-Generated Health Data in Care Delivery and Research through 2024,'' The Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, p. 5 (Jan. 2018), *https://www.healthit.gov/sites/default/files/onc_pghd_final_white_paper.pdf; see also* Jolaade Kalinowski, et al., ''Smart device ownership and use of social media, wearable trackers, and health apps among Black women with hypertension in the United States,'' JMIR Cardio (pre-print), *https://preprints.jmir.org/preprint/59243.*

[196] *See* ''Conceptualizing a Data Infrastructure for the Capture, Use, and Sharing of Patient-Generated Health Data in Care Delivery and Research through 2024,'' *supra* note 195, p. 1; Asos Mahmood, et al., ''mHealth Apps Use and Their Associations With Healthcare Decision-Making and Health Communication Among Informal Caregivers: Evidence From the National Cancer Institute's Health Information National Trends Survey,'' American Journal of Health Promotion, p. 40–52 (Jan. 2024), *https://journals-sagepub-com.hhsnih.idm.oclc.org/doi/10.1177/08901171231202861.*

[197] *See* 88 FR 75191 (Nov. 1, 2023); Ritu Agarwal, et al., ''Augmenting physicians with artificial intelligence to transform healthcare: Challenges and opportunities,'' Journal of Economics & Management Strategy, p. 360–374 (Mar. 2024), *https://onlinelibrary-wiley-com.hhsnih.idm.oclc.org/doi/10.1111/jems.12555;* Becca Beets, et al., ''Surveying Public Perceptions of Artificial Intelligence in Health Care in the United States: Systematic Review,'' Journal of Medical internet Research (2023), *https://doi.org/10.2196/40337.*

[198] Michael E. Matheny, et al., ''Artificial Intelligence in Health Care: A Report from the National Academy of Medicine,'' Journal of the American Medical Association, p. 509–10 (2020), *https://jamanetwork-com.hhsnih.idm.oclc.org/journals/jama/fullarticle/2757958.*

[199] ''2023 HIMSS Healthcare Cybersecurity Survey,'' Healthcare Information and Management Systems Society, p. 19 (Mar. 1, 2024), *https://www.himss.org/sites/hde/files/media/file/2024/03/01/2023-himss-cybersecurity-survey-x.pdf.*

[200] *Id.* at 16; Generative AI is a type of software that ''uses statistical models that generalize the patterns and structures of existing data to either reorganize existing data or create new content.'' ''Risk In Focus: Generative A.I. And The 2024 Election Cycle,'' Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security, *https://www.cisa.gov/sites/default/files/2024-05/Consolidated_Risk_in_Focus_Gen_AI_ElectionsV2_508c.pdf.*

[201] ''2023 HIMSS Healthcare Cybersecurity Survey,'' *supra* note 199, p. 22.

[202] *See* Lizzie Roehrs, ''CSL Professor explores DNA as data storage,'' University of Illinois Urbana-Champaign The Grainger College of Engineering Coordinated Science Laboratory (Aug. 25, 2020), *https://csl.illinois.edu/news-and-media/csl-professor-explores-dna-data-storage;* Cheng Kai Lim, et al., ''A biological camera that captures and stores images directly into DNA,'' nature communications (July 3, 2023), *https://www.nature.com/articles/s41467-023-38876-w;* Devasier Bennet, et al., ''Current and emerging opportunities in biological medium-based computing and digital data storage,'' Nano Select, p. 883 (May 2022), *https://doi-org.hhsnih.idm.oclc.org/10.1002/nano.202100275.*

[203] 88 FR 75191 (Nov. 1, 2023).

[204] *Id.* at 75214.

[205] *See* ''HHS Artificial Intelligence (AI) Strategy: AI Council & AI Community of Practice,'' U.S. Department of Health and Human Services (June 6, 2024), *https://www.hhs.gov/programs/topic-sites/ai/strategy/index.html;* ''About the HHS Office of the Chief Artificial Intelligence Officer (OCAIO),'' U.S. Department of Health and Human Services (June 6, 2024), *https://www.hhs.gov/programs/topic-sites/ai/ocaio/index.html; see also* ''Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence,'' M–24–10, Office of Management and Budget, Executive Office of the President (Mar. 28, 2024), *https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf.*

[206] *See, e.g.,* 89 FR 37522, 37642 (May 6, 2024) and 89 FR 1192, 1244 (Jan. 9, 2024).

[207] John Riggi, ''The importance of cybersecurity in protecting patient safety,'' American Hospital Association Center for Health Innovation, *https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety*; In 2016, PHI was valued at 50 times the worth of financial information on the black market. Diane Doebele Koch, ''Is the HIPAA Security Rule Enough to Protect Electronic Personal Health Information (PHI) in the Cyber Age?'' Journal of Health Care Finance, p. 22 (Spring 2016) (citing Beth Kutscher, ''Healthcare underspends on Cybersecurity as attacks accelerate,'' Modern Healthcare (Mar. 3, 2016), *https://www.modernhealthcare.com/article/20160303/NEWS/160309922/healthcare-underspends-on-cybersecurity-as-attacks-accelerate.*); ''New Dangers in the New World: Cyber Attacks in the Healthcare Industry,'' *supra* note 135, p. 3 (''[. . .] stolen medical data sells for 10–20 times more than credit card data.'').

valuable than credit card data, enabling cybercriminals to extract as much as [$1,000] per stolen medical record.'' [208] Before this shift to an interconnected electronic system, lost or misplaced paper records or even a laptop could lead to a breach of unsecured PHI affecting hundreds or thousands of individuals.[209] While a breach of that size remains significant, unauthorized access to a single workstation today could lead to a breach that affects millions of individuals because of the increase in interconnectivity.[210]

Between 2018 and 2023, the number of breaches of unsecured PHI reported to the Department grew at an alarming rate (100 percent increase), as did the number of individuals affected by such breaches (950 percent increase).[211] The reports reflect rampant escalation of cyberattacks using hacking (260 percent increase) and ransomware (264 percent increase).[212] Based on reports made to OCR, in 2022, approximately three-fourths of the breaches of unsecured PHI affecting 500 or more individuals were the result of hacking of electronic equipment or a network server.[213] In 2023, over 160 million individuals were affected by breaches involving the PHI of 500 or more individuals—a new record. We anticipate that 2024 will surpass that record, particularly in light of the estimate provided by a large covered entity regarding the number of individuals affected by a breach of its subsidiary.[214]

In 2023, the Federal Bureau of Investigation's internet Crime Complaint Center received almost 250 reports of ransomware affecting the Healthcare and Public Health sector, the most of any of the 16 identified infrastructure sectors.[215] The Healthcare and Public Health sector has been the most targeted critical infrastructure sector since at least as far back as 2015.[216] Between 2015 and 2019, cyberattacks on health care organizations increased by 125 percent.[217] And between 2022 and 2023, ransomware attacks against the U.S. health care sector increased 128 percent.[218]

Many people, including regulated entities, inaccurately believe that only large regulated entities that maintain electronic records about millions of individuals are likely to face a cyberattack, and thus that it is less important for smaller regulated entities to invest resources in cybersecurity.[219] In fact, smaller regulated entities may also be the target of, or adversely affected by, cybercrime, partly because of the interconnectedness of health care and partly because they are less likely to have invested in cybersecurity, making them easier targets.[220]

As explained in a recent national security memorandum, cybercriminals are targeting critical infrastructure (*i.e.,* the physical and virtual assets and systems so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, or national public health or safety), and their activities may be tolerated or enabled by other countries.[221] Thus, it is essential that the Department and regulated entities take steps to safeguard health care infrastructure and ePHI.

External actors are not the only, or even the greatest, threat to the security of ePHI. According to a recent study, insiders were the second leading cause of breaches in the health care sector in 2023, exceeded only by ''miscellaneous errors,'' such as misdelivery.[222] For example, a recent settlement resolved an OCR investigation involving the theft and sale of the ePHI of more than 12,000 patients by an employee of a large health care system.[223] In another example, security guards at a large health care provider were alleged to have used their login credentials to inappropriately access ePHI.[224] Thus, it is critical that regulated entities improve their cybersecurity posture to protect not only against external threats but also

[208] Gilbert Munoz-Cornejo, et al., ''Analyzing the urban-rural divide: the role of location, time, and breach characteristics in U.S. hospital security incidents, 2012–2021,'' Discover Health Systems (June 17, 2024), *https://link.springer.com/article/10.1007/s44250-024-00105-6#:~:text=Specifically%2C%20our%20study%20shows%20that,trend%20of%20breaches%20over%20time.*

[209] Lynne Coventry, et al., ''Cybersecurity in healthcare: A narrative review of trends, threats and ways forward,'' Maturitas, p. 46 (July 2018), *https://www.maturitas.org/article/S0378-5122(18)30165-8/abstract.*

[210] *Id.*

[211] *See* ''Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,'' *supra* note 10.

[212] *Id.*

[213] ''Annual Report to Congress on Breaches of Unsecured Protected Health Information: For Calendar Year 2022,'' Office for Civil Rights, U.S. Department of Health and Human Services, p. 8–9 (2022), *https://www.hhs.gov/sites/default/files/breach-report-to-congress-2022.pdf.*

[214] Change Healthcare is a health care clearinghouse and a subsidiary of UnitedHealth Group, *https://www.changehealthcare.com/.* On the morning of Feb. 21, 2024, Optum (another subsidiary of UnitedHealth Group) reported that it was ''experiencing enterprise-wide connectivity issues.'' By that afternoon, the announcement changed to a ''network interruption related to a cyber security issue'' and explained that ''[o]nce [Change Healthcare] became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact.'' *See* ''Optum Solution Status,'' Optum, Inc., UnitedHealth Group, *https://solution-status.optum.com/incidents/hqpjz25fn3n7* (last accessed on July 16, 2024). On Mar. 13, 2024, the Department announced that it would be initiating an investigation into the incident. *See* Letter from OCR Director Melanie Fontes Rainer to Colleagues (Mar. 13, 2024), *https://www.hhs.gov/sites/default/files/cyberattack-change-healthcare.pdf.* Andrew Witty, UnitedHealth Group Chief Executive Officer, in his testimony to Congress, estimated that the breach of Change Healthcare may involve the PHI of one-third of Americans. ''Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next,'' Subcommittee on Oversight and Investigations of the Committee on Energy and Commerce, Hearing Before the Committee on Finance (May 1, 2024), *https://www.finance.senate.gov/hearings/hacking-americas-health-care-assessing-the-change-healthcare-cyber-attack-and-whats-next.* Change Healthcare filed its breach report with the Department on July 19, 2024. ''Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,'' *supra* note 10. Change Healthcare's breach report currently identifies 100 million individuals as the ''approximate number of individuals affected.'' *https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.* However, Change Healthcare is still determining the number of individuals affected. The posting on the HHS Breach Portal will be amended if Change Healthcare updates the total number of individuals affected by this breach. ''Change Healthcare Cybersecurity Incident Frequently Asked Questions,'' Office for Civil Rights, U.S. Department of Health and Human Services, *https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html.*

[215] ''internet Crime Report,'' internet Crime Complaint Center, Federal Bureau of Investigation, p. 13 (2023), *https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf.*

[216] ''Report on Improving Cybersecurity In The Health Care Industry,'' *supra* note 117, p. 16.

[217] Chon Abraham, et al., ''Muddling through cybersecurity: Insights from the U.S. healthcare industry,'' *supra* note 116, p. 539–548, 540.

[218] ''Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double,'' The Cyber Threat Intelligence Integration Center, Office of the Director of National Intelligence (Feb. 28, 2024), *https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf.*

[219] ''Report on Improving Cybersecurity In The Health Care Industry,'' *supra* note 117, p. 14.

[220] *Id.*

[221] Presidential Memorandum on National Security Memorandum on Critical Infrastructure Security and Resilience *supra* note 11.

[222] ''2024 Data Breach Investigations Report: Healthcare Snapshot,'' Verizon Business, p. 12 (May 1, 2024) (The report describes misdelivery as sending information to the wrong recipient, whether by electronic or physical means), *https://www.verizon.com/business/resources/reports/dbir/2024/industries-intro/healthcare-data-breaches/.*

[223] Press release, ''HHS' Office for Civil Rights Settles Malicious Insider Cybersecurity Investigation for $4.75 Million,'' Office for Civil Rights, U.S. Department of Health and Human Services (Feb. 6, 2024), *https://www.hhs.gov/about/news/2024/02/06/hhs-office-civil-rights-settles-malicious-insider-cybersecurity-investigation.html.*

[224] Press release, ''Snooping in Medical Records by Hospital Security Guards Leads to $240,000 HIPAA Settlement,'' Office for Civil Rights, U.S. Department of Health and Human Services (June 15, 2023), *https://www.hhs.gov/about/news/2023/06/15/snooping-medical-records-by-hospital-security-guards-leads-240-000-hipaa-settlement.html.*

internal ones, and both intentional and accidental breaches.

Emergencies or other occurrences can affect the security of ePHI without an intentional act. For example, in 2024, CrowdStrike released a defective update for its software on computers running Microsoft Windows.[225] This update affected the ability of regulated entities to access the ePHI of millions of individuals for varying periods of time. During this time, ePHI was unavailable, meaning that one of the key prongs of the security triad of confidentiality, integrity, and availability was affected.[226] Because of the increased digitization of PHI, it is, for example, essential that covered health care providers engage in thoughtful contingency planning that considers how they will proceed in the event that they are unable to access ePHI in their EHRs. Additionally, threat actors will often seek to take advantage of such incidents. As reported by a large subcontractor of a business associate, less than a week after the outage, the company ''observed threat actors leveraging the event to distribute'' ransomware.[227] The environment in which health care is delivered, the way in which it is delivered, and the manner in which related information is collected all mean that regulated entities must consider a different approach to operational continuity and resiliency in the face of such challenges. Additionally, they must be wary of the potential for bad actors to attempt to take advantage of such events.

C. Regulated Entities' Compliance With the Requirements of the Security Rule Is Inconsistent

Despite the proliferation of cybersecurity standards, guidelines, best practices, methodologies, procedures, and processes and the documented increase in unauthorized uses and disclosures of ePHI, many regulated entities have been slow to strengthen their security measures to protect ePHI and their information systems that create, receive, maintain, or transmit it in this new environment.[228] Among the reasons for this are the rapid pace of EHR adoption and digitization of health care, increased connectivity and use of cloud-based infrastructures, limited competition and a stable customer base, limited operating margins, and a failure to invest in cybersecurity infrastructure.[229] For example, regulated entities continue to rely on legacy systems and software that are unsupported by manufacturers, which means that the manufacturers no longer provide security patches or other updates to address security threats and vulnerabilities.[230] In a 2021 survey of health care cybersecurity professionals, 73 percent reported having legacy operating systems.[231] This apparent lack of urgency in adopting new, supported operating systems has serious implications for the confidentiality, integrity, and availability of ePHI.

In addition, many regulated entities fail to invest adequate resources in cybersecurity. Far too many regulated entities do not view cybersecurity as a necessary component of their operations that allows them to fulfill their health care missions. Anecdotal evidence suggests that senior management often lacks awareness of cybersecurity, including both threats and methods for protecting against such threats.[232] ''A lack of maturity and effectiveness of the [information technology] function is evident when healthcare organizations fail to maintain a current inventory of sensitive and valuable data and where those reside.'' [233] While maintaining an accurate and thorough inventory of technology assets is not currently an explicit requirement of the Security Rule, it is clearly a fundamental component of conducting a risk analysis and many of the other existing requirements.[234] And yet, based on the Department's experience, many regulated entities are not maintaining such an inventory. At least in part because of senior management's lack of cybersecurity awareness, many fail to invest or fail to invest appropriately in cybersecurity infrastructure.[235] Given the vulnerability of ePHI and the information systems of regulated entities and the potential effects of cyberattacks on patient safety and the delivery of health care, it is important that regulated entities prioritize such investments.[236]

The security of ePHI also is at risk because, despite our explanation of the Security Rule's structure in 2003,[237] regulated entities are not fully complying with the standards and implementation specifications. From 2016 to 2017, the Department conducted audits of 166 covered entities and 41 business associates regarding compliance with selected provisions of the HIPAA Rules, including the required implementation specifications for risk analysis [238] and risk management.[239] The Department found that most regulated entities failed to implement the Security Rule requirements for risk analysis and risk management, requirements that are fundamental to protecting the confidentiality, integrity, and availability of ePHI.[240] While most of the audited business associates reported not having experienced any breaches of unsecured PHI, we found that those that

[225] ''Remediation and Guidance Hub: Falcon Content Update for Windows Hosts,'' CrowdStrike, *https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/.*

[226] *See* ''Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events,'' NIST Special Publication 1800–26A, National Institute of Standards and Technology, U.S. Department of Commerce, p. 1 (Dec. 2020), *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-26.pdf.*

[227] ''Likely eCrime Actor Uses Filenames Capitalizing on July 19, 2024, Falcon Sensor Content Issues in Operation Targeting LATAM-Based CrowdStrike Customers,'' CrowdStrike Blog (July 20, 2024), *https://www.crowdstrike.com/blog/likely-ecrime-actor-capitalizing-on-falcon-sensor-issues/.*

[228] Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, p. 2 (explaining that NCVHS conducted an inquiry into whether compliance with the Security Rule had improved since the Department released the results of its 2016–2017 audit of selected provisions of the Security Rule and found that ''not much had changed''); ''Muddling through cybersecurity: Insights from the U.S. healthcare industry,'' *supra* note 116, p. 540 (''There is enough evidence to suggest that U.S. healthcare organizations lack a deliberate, organized, and comprehensive cyber-resilience strategy.'').

[229] *See* Susan Kiser, et al., ''Ransomware: Healthcare Industry at Risk,'' Journal of Business and Accounting, p. 65–66 (Fall 2021); Meghan Hufstader Gabriel, ''Data Breach Locations, Types, and Associated Characteristics Among US Hospitals,'' American Journal of Managed Care, p. 78 (Feb. 2018); ''Is the HIPAA Security Rule Enough to Protect Electronic Personal Health Information (PHI) in the Cyber Age?'' *supra* note 207, p. 20–23.

[230] Chris Hayhurst, ''On Guard: Staying Vigilant Against Medical Device Vulnerabilities,'' Biomedical Instrumentation & Technology, Volume 54, Issue 3, p. 169 (May/June 2020); ''Report on Improving Cybersecurity In The Health Care Industry,'' *supra* note 117, p. 2.

[231] ''2021 HIMSS Healthcare Cybersecurity Survey,'' Healthcare Information and Management Systems Society, p. 18 (Jan. 28, 2022), *https://www.himss.org/sites/hde/files/media/file/2022/01/28/2021_himss_cybersecurity_survey.pdf.*

[232] ''Muddling through cybersecurity: Insights from the U.S. healthcare industry,'' *supra* note 116, p. 543.

[233] *Id.* at 542.

[234] *See* 68 FR 8334, 8352 (Feb. 20, 2003). In the preamble to the 2003 Security Rule, the Department explained that it had determined that an inventory requirement was unnecessary because it is redundant of other requirements. We assumed that covered entities (and later all regulated entities) would have performed this activity by virtue of having implemented the security measures required under the security management process standard.

[235] ''Muddling through cybersecurity: Insights from the U.S. healthcare industry,'' *supra* note 116, p. 542–543.

[236] Eric C. Reese, ''Healthcare's cybersecurity stakes reach alarming levels,'' Health Facilities Management Magazine, Volume 76, Issue 8, p. 22 (Nov. 2022).

[237] 68 FR 8334, 8343 (Feb. 20, 2003).

[238] 45 CFR 164.308(a)(1)(ii)(A).

[239] 45 CFR 164.308(a)(1)(ii)(B); ''2016–2017 HIPAA Audits Industry Report,'' *supra* note 121, p. 4.

[240] ''2016–2017 HIPAA Audits Industry Report,'' *supra* note 121, p. 4.

had experienced a breach generally engaged in minimal or negligible efforts to address the risk analysis and risk management requirements.[241] According to the report, at that time only 14 percent of covered entities and 17 percent of business associates were ''substantially fulfilling their regulatory responsibilities to safeguard ePHI they [held] through risk analysis activities,'' [242] while 94 percent of covered entities and 88 percent of business associates ''failed to implement appropriate risk management activities sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.'' [243] The report specifically noted that the audit results were consistent with the findings of OCR's compliance reviews and complaint investigations.[244]

Recent enforcement actions provide evidence that the results of the 2016–2017 audits were not isolated cases. In 2023, OCR entered into seven resolution agreements with regulated entities after investigations indicated that they had potentially violated the Security Rule, constituting almost half of the total resolution agreements OCR entered into that year.[245] In each case, OCR's investigation found evidence of multiple potential violations. For example, in one case, a regulated entity did not detect an intrusion into its network until 20 months later when its files were encrypted with ransomware.[246] OCR's investigation found evidence of potential failures of the regulated entity to conduct a risk analysis or to sufficiently monitor information system activity. OCR also found evidence that the regulated entity may not have had policies and procedures in place to implement the requirements of the Security Rule to protect the confidentiality, integrity, and availability of ePHI.[247]

As another example, an OCR investigation of a large health care system found indications of multiple potential violations of the Security Rule, including failures by the regulated entity to conduct a risk analysis, monitor and safeguard its electronic information systems, and implement policies and procedures to record and examine activity in its electronic information systems containing ePHI.[248] The regulated entity was not only unable to prevent the cyberattack, but it was unaware the attack had occurred until two years later. This is despite the long-standing requirements of the Security Rule and the obligations imposed on regulated entities for risk analysis and risk management.

Despite the long-standing nature of the Security Rule and the proliferation of guidance documents from NIST, the Department, CISA, FTC, and others, regulated entities continue to fail to implement reasonable and appropriate security measures as required by the Security Rule.[249] For example, the Security Rule and NIST guidance have addressed encryption for data in transit and at rest for many years.[250] And yet, in the 2021 survey of health care cybersecurity professionals, only half of the respondents reported having implemented encryption for data in transit across the enterprise.[251] Similarly, according to its CEO, a large covered entity failed to deploy multi-factor authentication (MFA) throughout its enterprise and experienced a significant breach.[252] If this is accurate, it would run counter to long-standing provisions in both the Security Rule and NIST guidance; the Security Rule has required the implementation of appropriate access controls since 2003 and NIST recommends similar controls.[253]

As another example, based on OCR's investigation experience, some regulated entities are not developing and implementing compliant response plans for security incidents, including those that are breaches of unsecured ePHI under the Breach Notification Rule. Section 164.308(a)(6)(i) establishes the standard that requires regulated entities to implement policies and procedures to address security incidents, while 45 CFR 164.308(a)(6)(ii) includes the implementation specifications for that standard. This requirement, included in the 2003 Final Rule, aligns with the NIST Cybersecurity Framework version 2.0 requirement for incident management.[254] Similarly, NIST Cybersecurity Framework version 1.1 recommended the execution and maintenance of response processes and procedures to ensure response to detected cybersecurity incidents.[255] And yet, when OCR investigates the circumstances surrounding breach reports, OCR continues to find evidence that regulated entities have not implemented policies and procedures to detect and respond to security incidents, leading to significant time lapses between a ''successful'' security incident [256] and discovery of, and response to, the security incident.[257] Thus, based on the OCR's experience investigating and enforcing the Security Rule, the Department believes that many regulated entities would benefit from additional instruction in regulatory text regarding their compliance obligations to determine how to select security

[241] *Id.* at 11.

[242] *Id.* at 27.

[243] *Id.* at 30.

[244] *Id.* at 27 and 30.

[245] *See* ''OCR News Releases & Bulletins,'' Office for Civil Rights, U.S. Department of Health and Human Services, *https://www.hhs.gov/ocr/newsroom/index.html.*

[246] *See* Resolution Agreement, ''Doctors' Management Services, Inc.,'' Office for Civil Rights, U.S. Department of Health and Human Services (Oct. 31, 2023), *https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/dms-ra-cap/index.html;* Press Release, ''HHS' Office for Civil Rights Settles Ransomware Cyber-Attack Investigation,'' Office for Civil Rights, U.S. Department of Health and Human Services (Oct. 31, 2023), *https://www.hhs.gov/about/news/2023/10/31/hhs-office-civil-rights-settles-ransomware-cyber-attack-investigation.html; see also* ''Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,'' *supra* note 10.

[247] ''HHS' Office for Civil Rights Settles Ransomware Cyber-Attack Investigation,'' *supra* note 246.

[248] *See* Resolution Agreement, ''Montefiore Medical Center,'' Office for Civil Rights, U.S. Department of Health and Human Services (Nov. 17, 2023), *https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/montiefore/index.html;* ''HHS' Office for Civil Rights Settles Malicious Insider Cybersecurity Investigation for $4.75 Million,'' *supra* note 223.

[249] ''Muddling through cybersecurity: Insights from the U.S. healthcare industry,'' *supra* note 116, p. 541; ''Start with Security: A Guide for Business,'' *supra* note 17.

[250] *See* 45 CFR 164.312(a)(1) and (e)(1); PR.DS–1 and 2, ''Framework for Improving Critical Infrastructure Cybersecurity,'' Cybersecurity Framework (CSF) Version 1.1, National Institute of Standards and Technology, U.S. Department of Commerce (Apr. 16, 2018), *https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf;* PR.DS–01 and 02, ''The NIST Cybersecurity Framework (CSF) 2.0,'' *supra* note 15.

[251] ''2021 HIMSS Healthcare Cybersecurity Survey,'' *supra* note 231, p. 23.

[252] *See* ''Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next,'' *supra* note 214 (According to CEO Andrew Witty, intruders used compromised credentials to remotely access an application used to enable remote access to desktops, which did not have MFA.). The Department's investigation into the Change Healthcare breach is ongoing, and no conclusion has been reached with respect to its cause or whether Change Healthcare was in violation of the Security Rule.

[253] 45 CFR 164.308(a)(4)(ii)(B) and 164.312(a)(1); ''The NIST Cybersecurity Framework (CSF) 2.0,'' *supra* note 15; ''Framework for Improving Critical Infrastructure Cybersecurity,'' *supra* note 250.

[254] RS.MA, ''The NIST Cybersecurity Framework (CSF) 2.0,'' *supra* note 15.

[255] PR.IP–9, ''Framework for Improving Critical Infrastructure Cybersecurity,'' *supra* note 250.

[256] 45 CFR 164.304 (definition of ''Security incident''). The definition of security incident includes both attempted and successful incidents. A successful incident is one in which a threat actor is able to, without authorization, access, use, disclose, modify, or destroy information or interfere with system operations in an information system.

[257] *See, e.g.,* ''Montefiore Medical Center,'' *supra* note 248.

measures that are reasonable and appropriate for their circumstances.

We are also concerned that recent caselaw has not accurately set forth the steps regulated entities must take to adequately protect the confidentiality, integrity, and availability of ePHI, as required by the statute. Specifically, in the *University of Texas M.D. Anderson Cancer Center* v. *HHS* (''*M.D. Anderson*''), the U.S. Court of Appeals for the Fifth Circuit held, among other things, that the Security Rule does not say anything about how effective a mechanism for encryption must be, nor does it require that an encryption mechanism provide ''bulletproof protection'' of all systems containing ePHI.[258] Thus, under the court's interpretation, a regulated entity can meet its obligations under the Security Rule concerning encryption and decryption of ePHI by implementing a mechanism to do so, without regard for the effectiveness of the implementation.[259] Additionally, the court noted that the requirement for ''a mechanism'' does not ''prohibit a [regulated] entity from creating 'a mechanism' by directing employees to sign an [agreement] that requires the encryption of portable devices.'' [260] While the Department disagrees with the court's interpretation that merely requiring employees to sign an agreement to encrypt portable devices is sufficient to comply with its Security Rule obligations to implement a mechanism to encrypt and decrypt ePHI, the Department believes that additional clarity is warranted to ensure that regulated entities understand their obligation to have encryption mechanisms in place and deployed throughout the regulated entity's enterprise to ensure the confidentiality, integrity, and availability of ePHI.

Several technical safeguards currently require regulated entities to implement a ''mechanism'' as part of complying with the associated standard. Given that written policies and procedures alone are insufficient to protect ePHI, and the misinterpretation of what it means to implement a mechanism also could lead to inadequate protection of ePHI, the Department believes that the Security Rule must be revised, consistent with its statutory mandate, as discussed in greater detail above.

D. It Is Reasonable and Appropriate To Strengthen the Security Rule To Address the Changes in the Health Care Environment and Clarify the Compliance Obligations of Regulated Entities

1. Congress and the Department Anticipated That Security Standards Safeguards Would Evolve To Address Changes in the Health Care Environment

By requiring that regulated entities maintain reasonable and appropriate safeguards to protect against reasonably anticipated threats or hazards or unauthorized uses or disclosures of ePHI, Congress clearly anticipated that the administrative, physical, and technical safeguards implemented to protect the security of ePHI would need to change in response to changes in the environment in which health care is provided.[261] As the health care environment and the operations of regulated entities evolve, so must the protections for ePHI and the information systems used to create, receive, maintain, or transmit it. For example, regulated entities must be expected to adopt safeguards that address new risks to the security of ePHI, such as those posed by maintaining ePHI in the cloud; the connection of medical devices and other technology to networks; and the connection of information systems used to create, receive, maintain, or transmit ePHI to the same networks as those do not perform such activities. After all, it is reasonable to anticipate that there will be new threats or hazards to ePHI or efforts by unauthorized persons to use or disclose such ePHI in an increasingly connected environment.

By design, the Security Rule sets a national floor for the security measures that regulated entities are required to implement to protect the confidentiality, integrity, and availability of ePHI. In 2003, the Department opted to frame the standards in terms that were as generic as possible and in a manner that enabled the standards to be met through various approaches or technologies to ensure that regulated entities had the flexibility to determine how best to protect the confidentiality, integrity, and availability of ePHI based on their specific circumstances.[262] When we extended the Security Rule in 2013 to directly apply to business associates in accordance with the HITECH Act,[263] the Department acknowledged that some business associates might not have engaged in the formal administrative safeguards required by the Security Rule, and we made it clear that business associates would be expected to do so going forward.[264] Despite the changes in the health care environment between 2003 and 2013, the Department made minimal changes to the Security Rule at that time because we believed that the compliance obligations of regulated entities were clear and well-understood. In fact, when a commenter recommended that the Department remove the ''addressable'' designation from the Security Rule because it leads to ambiguity in the rule's application, we declined to do so at that time because we were concerned that it would reduce the rule's scalability and flexibility.[265] However, as we noted in 2003, the rule's flexibility of approach is primarily provided for in paragraph (b)(2) of 45 CFR 164.306 and in the standards themselves.[266] The addressability feature merely provided an added level of flexibility [267] in a way that the Department now believes is inadequate to ensure that regulated entities implement reasonable and appropriate security safeguards.

Changes to the health care environment and the operations of regulated entities have increased the importance of implementing strong security measures to protect ePHI and the information systems that create, receive, maintain, or transmit it. While we recognize the burdens posed by such implementation on regulated entities, there is also a clearly documented increase in the number of breaches of unsecured PHI and instances of cybercriminals accessing ePHI without authorization at regulated entities. The changes to the health care environment, including the increase in breaches and cyberattacks, and operations of regulated entities have made it increasingly likely that unauthorized persons will seek to obtain ePHI and disrupt the U.S. health care system. Additionally, the clearly documented failure of regulated entities to fully implement the policies and procedures required by the Security Rule and apply the required security measures throughout their operations has caused the Department to question whether the existing Security Rule should be revised to clarify and strengthen the obligations of regulated entities and revisit our

[258] *University of Texas M.D. Anderson Cancer Center* v. *U.S. Department of Health and Human Services,* 985 F.3d 472, 478 (5th Cir. 2021).

[259] *Id.*

[260] *Id.*

[261] Sec. 1173(d)(2)(B) of Pub. L. 104–191, 110 Stat. 2026 (Aug. 21, 1996) (codified at 42 U.S.C. 1320d–2).

[262] 68 FR 8334, 8336 (Feb. 20, 2003).

[263] 42 U.S.C. 17931(a); 78 FR 5566 (Jan. 25, 2013).

[264] 78 FR 5566 (Jan. 25, 2013).

[265] *Id.* at 5591.

[266] *See* 68 FR 8334, 8341 (Feb. 20, 2003).

[267] *Id.* at 8344.

decision from 2013.[268] In many cases involving a breach of ePHI that OCR has investigated, a breach may not have occurred, or would have been less widespread and disruptive, had the regulated entities fully implemented the provisions of the Security Rule.[269]

2. NCVHS Believes That the Security Standards Evolve To Address Changes in the Health Care Environment

The Department is not alone in believing that the Security Rule should be strengthened to address concerns about whether -regulated entities are sufficiently protecting the confidentiality, integrity, and availability of ePHI. An inquiry conducted by NCVHS between July 2021 and September 2023 reached the same conclusion.[270] During this inquiry, NCVHS listened to the testimony of cybersecurity experts and Department officials. The experts and Department officials ''consistently voiced their concerns about the major increase in incidents and, in particular, the widespread lack of robust risk analysis on the part of covered entities and business associates that would lead to prior planning for, and mitigation of, a range of cybersecurity threats.'' [271] In response to this inquiry and consistent with their statutory mandate,[272] NCVHS transmitted two letters to the Secretary with recommendations for improving cybersecurity practices in the health care industry, including recommendations for modifying the Security Rule.[273] As part of the explanation for its concerns, NCVHS cited a 2021 survey of acute and ambulatory care organizations that found only 32 percent of those organizations had a comprehensive security program, while only 26 percent of the long-term and post-acute care facilities met the minimum security requirements.[274] Specifically, NCVHS made the following recommendations for improvements to the Security Rule:

- Eliminate from the addressable implementation specifications the choice not to implement a specification or alternative, and instead require regulated entities to implement the specification or adopt a documented reasonable alternative.[275]
- Include specific minimum cybersecurity hygiene requirements that are reflective of modern industry best practices, including designation of a qualified information security official, elimination of default passwords, adoption of MFA, institution of offline backups, installation of critical patches within a reasonable time, and transparency of impact and vulnerability disclosures.[276]
- Require that regulated entities implement a security program and that they implement standard minimum security controls.[277]
- Require that regulated entities adopt a risk-based approach in their security program.[278]
- Require that regulated entities perform a risk analysis in a manner that conforms with guidance from NIST and CISA.[279]
- Define compensating controls more specifically and provide a wider range of examples that apply to a greater variety of types of entities.[280]
- Reinforce the need for regulated entities to account for AI systems and data within their risk analysis for all and any new technology.[281]
- Establish a consistent floor for cyber incident reporting and harmonize such requirements with incident reporting provisions applicable to health care critical infrastructure actors and health care Federal contractors.[282]

The Department, in drafting this NPRM, relied on the recommendations of NCVHS, OCR's enforcement experience, news reports, and our assessment of the environment. Consistent with NCVHS' recommendation to revisit the Security Rule's classification of some implementation specifications as ''addressable,'' the Department also believes that it is appropriate to revisit our decision regarding the amount of flexibility regulated entities have in determining reasonable and appropriate safeguards, as described above. Based on OCR's experience in investigations and audits, we believe that regulated entities would benefit from greater specificity in the Security Rule. The Department has provided extensive guidance on questions to consider when adopting and implementing security measures and ways to comply with the Security Rule,[283] as directed by the HITECH Act. And yet, despite this proliferation of guidance, regulated entities continue not to comply. For example, despite the explanation in 45 CFR 164.306(d) about addressable implementation specifications and the notable changes in the environment in which health care is provided, we are concerned that some regulated entities proceed as if compliance with an addressable implementation specification is optional—and that where there is an addressable implementation specification, that compliance with the relevant standard is also optional. That interpretation is incorrect and weakens the cybersecurity posture of regulated entities. We believe that compliance with the implementation specifications currently designated as addressable is not—and should not be—optional, particularly in light of the shift to an interconnected and cloud-based environment and a significant increase in the number of breaches of unsecured PHI from both internal and external actors, regardless of the regulated entity's specific circumstances. Thus, we believe that it is necessary to strengthen the Security Rule to reflect the changes in the health care environment and the evolution of

[268] *See* ''2016–2017 HIPAA Audits Industry Report,'' *supra* note 121, p. 4 (''[M]ost covered entities failed to meet the requirements for other selected provisions in the audit, such as adequately safeguarding protected health information (PHI) [. . .] OCR also found that most covered entities and business associates failed to implement the HIPAA Security Rule requirements for risk analysis and risk management.''); ''Enforcement Highlights,'' Office for Civil Rights, U.S. Department of Health and Human Services, *https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.*

[269] *See, e.g.,* ''Montefiore Medical Center,'' *supra* note 248; ''Doctors' Management Services, Inc.,'' *supra* note 246.

[270] Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, p. 2 (detailing the inquiry undertaken by NCVHS into the scope and breadth of security risks and how to best address those challenges).

[271] *Id.*

[272] *See* 42 U.S.C. 1320d–1(f).

[273] *See* Letter from NCVHS Chair Jacki Monson (2022), *supra note 123;* Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123.

[274] *See* Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123, p. 4 (citing a survey performed by a College of Healthcare Information Management Executives (CHIME) as explained at Jill McKeon, ''32% of Healthcare Organizations Have a Comprehensive Security Program,'' Health IT Security (Nov. 22, 2021), *https://healthitsecurity.com/news/32-of-healthcare-organizations-have-a-comprehensive-securityprogram*).

[275] *See* Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123, p. 4; *see also* Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 1.

[276] *See* Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123, p. 5–10; *see also* Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 2.

[277] Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 1–4.

[278] *Id.* at Appendix p. 4–5.

[279] *Id.* at Appendix p. 4–6.

[280] *Id.* at Appendix p. 6–7.

[281] *Id.* at Appendix p. 7–8.

[282] *Id.* at 9–10.

[283] The Department has issued, among other things, a video presentation on trends in real world cyberattacks, a cybersecurity checklist and infographic, guidance on ransomware, a crosswalk with the NIST CSF, and an ongoing series of newsletters on various topics pertaining to cybersecurity. *See* ''Cyber Security Guidance Material,'' Office for Civil Rights, U.S. Department of Health and Human Services, *https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html.*

technology and to underscore that compliance with all of our proposals, if finalized, is required.

3. A Strengthened Security Rule Would Continue To Be Flexible and Scalable While Providing Regulated Entities With Greater Clarity

The Security Rule's fundamental flexibility and scalability generally would remain should the proposals in this NPRM be adopted. However, we are proposing to reduce that flexibility to better strengthen protections and address the changed nature of the environment in which health care is provided. The Department is also proposing in this NPRM to strengthen the Security Rule by providing greater clarity regarding the nature of its flexibility and scalability and the Department's expectations, as requested by regulated entities and other stakeholders. In fact, in response to a request for information published in 2022,[284] several commenters urged the Department to propose regulations that establish a single set of clear standards for regulated entities, raise the floor for security requirements and expectations, and encourage regulated entities to safeguard ePHI while maintaining flexibility and scalability. Commenters also encouraged the Department to rely on commonly available, non-proprietary frameworks that allow regulated entities to adopt critical security measures. We believe that our proposals are consistent with those recommendations.

Under the proposal, regulated entities would retain the ability to determine the security measures that are reasonable and appropriate to fulfill the required standards and implementation specifications, taking into consideration the factors listed at proposed 45 CFR 164.306(b)(2). In fact, the NPRM, if adopted as proposed, would add to the rule's flexibility and scalability by adding a new factor for regulated entities to consider when determining the reasonable and appropriate security measures.[285]

Additionally, if modifications are adopted as proposed, the Security Rule would remain flexible and scalable by retaining broad standards with which regulated entities could comply in a variety of ways. In 2003, the 13 implementation specifications that the Security Rule requires were considered so basic that no covered entity could effectively protect ePHI without implementing them.[286] While the Department agrees that these implementation specifications remain essential, we no longer believe that they are sufficient to address the risks to ePHI today. Rather, regulated entities must do more to ensure the confidentiality, integrity, and availability of ePHI today because of the changes in the environment in which health care is provided, how ePHI is maintained, the level of connectivity between information systems, and the technological sophistication of bad actors.

We acknowledged in 2003 and again acknowledge here that ''there is no such thing as a totally secure system that carries no risks to security.'' [287] We posited at that time that Congress intended to set an ''exceptionally high goal for the security of [ePHI],'' while also recognizing that securing ePHI did not require that covered entities do so without regard for the cost.[288] However, we also made clear that a covered entity is required to implement adequate security measures and that cost was but one factor for a covered entity to consider when determining what constituted appropriate security measures.[289] As we noted, ''Cost is not meant to free covered entities from this responsibility.'' [290] In the 2013 Omnibus Rule, we further explained that ''[regulated entities] have the flexibility to choose security measures appropriate for their size, resources, and the nature of the security risks they face, enabling them to reasonably implement any given Security Rule standard. [. . .] Thus, the costs of implementing for [. . .] business associates will be proportional to their size and resources.'' [291] We continue to believe that this is the case. Additionally, as discussed above, there is a significant cost associated with breaches and unauthorized access—financial, reputational (for both the individual and the regulated entity), and more. Thus, we believe that the standards and implementation specifications that we propose in this NPRM are the minimum that regulated entities should be doing to protect the security of ePHI and lower the costs associated with breaches and other incidents.

4. Small and Rural Health Care Providers Must Implement Strong Security Measures To Provide Efficient and Effective Health Care

The statute requires that we consider the ''needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary).'' [292] We recognize that small and rural health care providers may have needs and capabilities that differ from those of other regulated entities. For example, small health care providers and rural health care providers are often located at a greater distance from other health care providers.[293] It may be more challenging for them to attract and retain clinicians and administrative support staff.[294] They also face difficulty attracting and retaining security experts and must make difficult decisions regarding investments in competing priorities.[295] Often, preparation for security incidents or other occurrences that adversely affect the confidentiality, integrity, or availability of ePHI is neglected in favor of other priorities, putting small and rural health care providers at greater risk for such an occurrence.[296]

We continue to believe that it is just as important for small and rural health care providers to implement strong security measures as it is for larger health care providers and other categories of regulated entities. According to experts, ''Cybercriminals go after small businesses, especially those in the healthcare industry,

[284] *See* 87 FR 19833 (Apr. 6, 2022).

[285] *See* proposed 45 CFR 164.306(b)(2)(v).

[286] 68 FR 8334, 8336 (Feb. 20, 2003).

[287] *Id.* at 8346.

[288] *Id.* At that time, the Security Rule applied directly only to covered entities. As discussed above, Congress later extended the application of the Security Rule directly to business associates.

[289] 68 FR 8334, 8343 (Feb. 20, 2003).

[290] *Id.*

[291] 78 FR 5566, 5589 (Jan. 25, 2013).

[292] 42 U.S.C. 1320d–2(d)(1)(A)(v).

[293] *See* ''Why Health Care is Harder to Access in Rural America,'' U.S. Government Accountability Office (May 16, 2023) (When local hospitals close in rural areas, residents have to travel more than 20 miles further to receive common health care and 40 miles further to receive less common health care, such as substance use disorder treatment. Such rural areas generally have fewer health care providers overall.), *https://www.gao.gov/blog/why-health-care-harder-access-rural-america.*

[294] *See* ''A National Staffing Emergency in Rural Health Care,'' American Hospital Association (Dec. 19, 2023), *https://www.aha.org/advancing-health-podcast/2023-12-20-national-staffing-emergency-rural-health-care.*

[295] *See* Debi Primeau, ''How Small Organizations Handle HIPAA Compliance,'' Journal of the American Health Information Management Association, Volume 88, Issue 4, p. 18–21, 19 (Apr. 2017); Kat Jercich, ''Rural hospitals are more vulnerable to cyberattacks—here's how they can protect themselves,'' Healthcare IT News (Sept. 8, 2021); *see also* Tami Lichtenberg, ''Recovering from a Cybersecurity Attack and Protecting the Future in Small, Rural Health Organizations'' (Oct. 4, 2023), *https://www.ruralhealthinfo.org/rural-monitor/cybersecurity-attacks.*

[296] *See* ''How Small Organizations Handle HIPAA Compliance,'' *supra* note 295, p. 19; ''Rural hospitals are more vulnerable to cyberattacks—here's how they can protect themselves,'' *supra* note 295.

because they are easy targets.'' [297] In 2017, 93 percent of small rural and critical access hospitals and 86 percent of physician offices relied on health IT to inform their clinical practice.[298] And yet, small health care providers are less likely than a larger organization to even have a designated security or compliance officer.[299] Smaller practices and rural and community facilities also may be more likely to rely on older technologies that are no longer supported by security patches and updates, including medical devices such as insulin pumps and pacemakers in which inaccuracies or errors could affect patient safety.[300] Thus, small health care providers ''are at the greatest risk of a breach. [. . .] Smaller, rural practice settings are especially high-risk target areas for a breach.'' [301] According to an expert who speaks to and works with health care providers on IT services and cybersecurity, small health care providers are ''more susceptible because they do not have a lot of the tools and security measures necessary to protect themselves.'' [302] For example, a critical access hospital in Colorado recovered from a cyberattack in 2019, but it required ''an incredible amount of staff time, many months of recovery efforts, and an enormous financial outlay to restore systems and prevent another attack.'' [303] In fact, the hospital estimates that ''it took a full year of a staff person's time to complete the recovery and protect the organization for the future.'' [304] These costs do not include the multiple ransoms paid to the attackers after the first set of keys did not unlock all of the data.[305]

Patients and communities have a critical need for health care providers, including rural hospitals and other rural health care providers, to be resilient and remain operational, which depends in part on the cybersecurity of their electronic information systems. For rural health care providers, especially hospitals, a breach can significantly affect an entire community.[306] Rural health care providers often are separated by significant distances, which can have real consequences for someone experiencing a medical emergency.[307] A recent study comparing hospital characteristics and operations of rural and urban hospitals that experienced ransomware attacks between 2016 and 2021 found that rural hospitals experienced large declines in inpatient admissions and Medicare revenue, similar to those experienced by urban hospitals.[308] The study also found that the decline in volume and revenue of hospital outpatient and emergency room visits was more pronounced among rural facilities.[309] In fact, in June 2023, a hospital in rural Illinois announced that it would close, in part because a 2021 cyberattack prevented it from submitting claims to health plans for months.[310] According to a local elected official, the hospital's closure would require some residents to travel approximately 30 minutes for the nearest emergency room and obstetrics services.[311] Thus, implementing security measures to maintain facility operations is critical to minimize or avoid disruptions to patient care and patient safety activities in such facilities. Consistent with these examples, the Department believes that small and rural health care providers are also viewed as potential targets by cybercriminals, and such providers need to implement strong cybersecurity measures to secure the ePHI in their possession. In fact, in June 2024, the Administration announced a collaboration with the private sector to provide additional cybersecurity resources for rural health care providers in recognition of the importance of protecting the security of ePHI created, received, maintained, or transmitted by such entities.[312] We believe this collaboration will provide small and rural health care providers with additional support, particularly when coupled with other resources described in greater detail below.[313] Thus, we believe that small and rural health care providers have both the need to comply with the proposals in this NPRM and the capability of doing so. Additionally, we believe that the NPRM would continue to provide all regulated entities, including small and rural health care providers, the ability to take into account their circumstances when determining which security measures are reasonable and appropriate.[314]

5. A Strengthened Security Rule Is Critical to an Efficient and Effective Health Care System

While the Security Rule generally continues to accomplish a primary goal of HIPAA,[315] the Department believes that it is essential to propose modifications to strengthen its protections for the confidentiality, integrity, and availability of ePHI to address the changing health care environment. We also believe it is important to clarify the obligations of regulated entities and emphasize the importance of protecting the confidentiality, integrity, and availability of ePHI. We believe that the proposed revisions would require regulated entities to consider and potentially modify their safeguards more regularly, which would better enable them to quickly respond to changes in the environment and be consistent with cybersecurity best practices. While we do not expect that compliance with the Security Rule will

[297] ''Too Small to Be Attacked by Cybercriminals? Not So Fast,'' Same-Day Surgery, Volume 43, Issue 7 (July 2019), *https://www.reliasmedia.com/articles/144561-too-small-to-be-attacked-by-cybercriminals-not-so-fast.*

[298] ''Percent of Hospitals, By Type, that Possess Certified Health IT,'' Health IT Quick-Stat #52 (Sept. 2018), *https://www.healthit.gov/data/quickstats/percent-hospitals-type-possess-certified-health-it;* ''Office-based Physician Electronic Health Record Adoption,'' Health IT Quick-Stat #50, *https://www.healthit.gov/data/quickstats/office-based-physician-electronic-health-record-adoption.*

[299] ''How Small Organizations Handle HIPAA Compliance,'' *supra* note 295, p. 19.

[300] *See id.*

[301] *Id.; see also* ''Recovering from a Cybersecurity Attack and Protecting the Future in Small, Rural Health Organizations,'' *supra* note 295.

[302] ''Too Small to Be Attacked by Cybercriminals? Not So Fast,'' *supra* note 297.

[303] ''Recovering from a Cybersecurity Attack and Protecting the Future in Small, Rural Health Organizations,'' *supra* note 295.

[304] *Id.*

[305] *Id.*

[306] *See, e.g.,* ''Fact Sheet: Biden-Harris Administration Bolsters Protections for Americans' Access to Healthcare Through Strengthening Cybersecurity,'' The White House (June 10, 2024), *https://www.whitehouse.gov/briefing-room/statements-releases/2024/06/10/fact-sheet-biden-harris-administration-bolsters-protections-for-americans-access-to-healthcare-through-strengthening-cybersecurity/;* ''How Do Ransomware Attacks Impact Rural Hospitals?,'' National Institute for Health Care Management Foundation, p. 1 (2024), *https://nihcm.org/assets/articles/FINAL-NIHCM-RI-Hannah-Neprash_2024-08-01-132728_ushq.pdf.*

[307] ''How Do Ransomware Attacks Impact Rural Hospitals?'' *supra* note 306, p. 2.

[308] *Id.*

[309] *Id.*

[310] Kevin Collier, ''An Illinois hospital is the first health care facility to link its closing to a ransomware attack,'' NBC News (June 12, 2023), *https://www.nbcnews.com/tech/security/illinois-hospital-links-closure-ransomware-attack-rcna85983.*

[311] *Id.*

[312] ''Fact Sheet: Biden-Harris Administration Bolsters Protections for Americans' Access to Healthcare Through Strengthening Cybersecurity,'' *supra* note 306.

[313] *See, e.g.,* ''Free Cybersecurity Services and Tools,'' Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security, *https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools;* ''Cyber Hygiene Services,'' Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security, *https://www.cisa.gov/cyber-hygiene-services;* ''Cybersecurity Resources for High-Risk Communities,'' Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security, *https://www.cisa.gov/audiences/high-risk-communities/cybersecurity-resources-high-risk-communities.*

[314] *See, e.g.,* 45 CFR 164.306.

[315] *See* sec. 261 of Pub. L. 104–191, 110 Stat. 2021 (Aug. 21, 1996), as amended by sec. 1104(a) of Pub. L. 111–148, 124 Stat. 146 (Mar. 23, 2010) (codified at 42 U.S.C. 1320d note).

prevent all breaches or interruptions in the confidentiality, integrity, or availability of ePHI, we believe that it will prevent many and enable regulated entities to identify, mitigate, and remediate the damage more quickly if there is a breach or other security incident, thereby reducing harm to individuals and the overall costs of such occurrences to regulated entities and to the U.S. health care system. As such, the proposed modifications would support a primary goal of HIPAA's Administrative Simplification provisions: improving the efficiency and effectiveness of the U.S. health care system by encouraging the development of health information systems through the establishment of uniform standards and requirements for electronic transmission of ePHI, including those for security.[316]

E. The Secretary Must Develop Standards for the Security of ePHI Because None Have Been Developed by an ANSI-Accredited Standard Setting Organization

HIPAA requires the Secretary to adopt standards that have been developed, adopted, or modified by a standard setting organization accredited by ANSI, except in certain circumstances.[317] For example, HIPAA permits the Secretary to develop standards where no relevant standards have been developed, adopted, or modified by an ANSI-accredited standard setting organization. In developing, adopting, or modifying a standard, the Secretary is required to consult with standard setting organizations, NCVHS, and with the appropriate Federal and State agencies.[318]

The statutory definition of the term ''standard'' applies only to standards for electronic transactions and data elements for such transactions that are appropriate for: (1) the financial and administrative transactions described in the statute; and (2) other financial and administrative transactions consistent with the goals of improving the operation of the health care system and reducing administrative costs, as determined appropriate by the Secretary.[319] Under HIPAA, security is not considered a financial or administrative transaction, or a data element of such transaction.[320] In the ''Health Insurance Reform: Standards for Electronic Transactions'' final rule in 2000, we explicitly adopted a broader definition of ''standard'' because we recognized that the statutory definition only applied to standards for financial and administrative transactions, despite the statute's requirement that the Secretary adopt standards addressing other matters, including privacy and security.[321] At that time, we explained that we adopted a broader definition of standard to accommodate the varying functions of the specific standards proposed in other HIPAA regulations.[322] For the same reason, we believe that it is appropriate to continue to rely on the regulatory definition of standard.[323]

As discussed above, in both 1998 and 2003, the Department determined that no comprehensive, scalable, and technology-neutral set of standards exists, and accordingly, we proposed and adopted a new standard.[324] In 2013, we made only minor modifications to the standards when we complied with explicit directions from Congress to apply the requirements of the Security Rule to business associates, so we did not need to consider whether an ANSI-accredited standard setting organization had adopted a comprehensive set of standards on the security for ePHI that was flexible, scalable, and technology-neutral.[325]

However, because we believe it is appropriate for us to consider modifying the Security Rule at this time for the reasons discussed above, we must again consider whether an ANSI-accredited standards setting organization has developed, adopted, or modified a standard relating to the security of ePHI. The Department continues to believe that any standard must be comprehensive, rather than piecemeal, as recommended by the ANSI Healthcare Informatics Standards Board.[326] We also continue to agree with the recommendation that the standards should be technology-neutral because security technology continues to evolve to keep pace with the evolution of technology more broadly. Additionally, the Security Rule must remain flexible and scalable to allow for consideration of the wide variety of regulated entities, enabling such entities to determine the reasonable and appropriate security measures for their circumstances by taking into account the factors specified by HIPAA.[327]

We are not aware of any standard setting organizations that are accredited by ANSI that have issued standards for the security of ePHI, let alone standards that are sufficiently comprehensive, flexible, scalable, and technology-neutral to enable regulated entities to take into account the HIPAA factors. For example, NIST has issued numerous publications addressing health care cybersecurity that are considered by NIST to be guidance, rather than standards. In fact, NIST is ANSI-accredited for only one standard.[328] And with the exception of publications that analyze the Security Rule, NIST's guidance does not specifically address the security of ePHI. CISA has issued cross-sector CPGs, but it is not ANSI-accredited. There may be other organizations that have set standards for the transmission of particular information, such as the secure transmission of images, but adopting such individual standards would not meet the Department's criteria. In this case, adoption of such standard would be far too granular and require the Department to revise the Security Rule at the same interval as the particular standard, which may be irregular. Additionally, given that the Department is limited to modifying each standard or implementation specification no more frequently than once every 12 months, this approach would be inefficient and could lead to a requirement that the Department update the Security Rule more than once a year, depending on when such individual standards or implementation specifications are revised. Even modifying the standards annually would require a significant investment of Department resources, not to mention the investment required of regulated entities to comply with an ever-changing set of requirements.

Additionally, in 2021, Congress amended the HITECH Act to require the Secretary to consider whether a regulated entity has adequately demonstrated that it had in place recognized security practices for a certain period of time.[329] Congress defined ''recognized security practices'' to include certain NIST publications; the approaches promulgated under

[316] *Id.*

[317] 42 U.S.C. 1320d–1(c)(1) and (2).

[318] 42 U.S.C. 1320d–1(c)(2)(B).

[319] *See* 42 U.S.C. 1320d(7) (definition of ''Standard'').

[320] *See* 42 U.S.C. 1320d–2(a)(1).

[321] 65 FR 50312, 50320 (Aug. 17, 2000); *see also* 42 U.S.C. 1320d–2(b), (c), and (d); sec. 264(c) of HIPAA.

[322] 65 FR 50312, 50320 (Aug. 17, 2000).

[323] 45 CFR 160.103 (definition of ''Standard'').

[324] 63 FR 43242, 43249 (Aug. 12, 1998); 68 FR 8334, 8341 (Feb. 20, 2003).

[325] 78 FR 5566, 5589–91, 5693–95 (Jan. 25, 2013).

[326] 63 FR 43249 (Aug. 12, 1998); 68 FR 8341 (Feb. 20, 2003).

[327] 42 U.S.C. 1320d–2(d)(1)(A).

[328] ''ANSI/NIST–ITL Standard,'' National Institute of Standards and Technology, U.S. Department of Commerce (Feb. 3, 2023), *https://www.nist.gov/programs-projects/ansinist-itl-standard*.

[329] *See* section 13412(a) of the HITECH Act, as amended by section 1 of Public Law 116–321, 134 Stat. 5072 (Jan. 5, 2021) (codified at 42 U.S.C. 17941(a)(1)).

section 405(d) of the Cybersecurity Act of 2015; ''and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities.'' [330] However, the HITECH Act amendment did not require the Secretary to accept a regulated entity's implementation of recognized security practices as an alternative to compliance with the Security Rule, nor did it provide that such implementation was sufficient to meet the security objectives of HIPAA or the HITECH Act. Accordingly, it is appropriate for the Department to develop and adopt its own standards to meet the statutory objective of ensuring the security of ePHI. The standards and implementation specifications proposed herein take into consideration not only those promulgated by NIST, but also guidelines, best practices, methodologies, processes, and procedures published by CISA, the HHS 405(d) program, CMS, State governments, and others. The proposals also enable regulated entities to adopt security measures that ensure the confidentiality, integrity, and availability of ePHI; protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI and unauthorized uses or disclosures of such ePHI; ensure compliance with the Security Rule by the workforce members of regulated entities, while also taking into account the technical capabilities of record systems used to maintain ePHI; the costs of such measures; the need for training users who have access to ePHI; the value of audit trails in computerized record systems; and the needs and capabilities of small and rural health care providers.

The Department has consulted with and relied on the recommendations of NCVHS in the formulation of this proposed rule [331] and intends to continue to engage in these consultations before finalizing the rule.[332] We also expect to consult with the National Uniform Billing Committee, the National Uniform Claim Committee, the Workgroup for Electronic Data Interchange, and the American Dental Association before finalizing this rule, as required by section 1172(c)(3)(A)(ii) of HIPAA.[333]

[330] *Id.*

[331] *See* Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123; Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123.

[332] 42 U.S.C. 1320d–1(f).

[333] 42 U.S.C. 1320d–1(c)(3)(A)(ii).

IV. Section-by-Section Description of the Proposed Amendments to the Security Rule

This section contains a description of the proposed amendments to the Security Rule and the Department's rationale for its proposals. As part of this rationale, we often include a discussion of best practices contained in previously published guidance documents issued by the Department, NIST, and other Federal agencies. We request comment on previously published guidance documents that are not discussed herein that were issued by the Department or other Federal agencies and contain best practices but may be relevant or applicable to regulated entities, including the names of and citations for such guidance documents. We do not propose to adopt referenced best practices as the standard or implementation specifications unless otherwise specified in the proposed regulatory text. Rather, we include such discussion to provide regulated entities with context for the aforementioned proposals. We recognize that regulated entities are of varying types and sizes and may be concerned that requiring the adoption of such best practices might not be appropriate for all. However, we request comment on whether we should require implementation of certain aspects of a particular guidance document. If so, please explain which aspect(s) we should require, the rationale, and information about the burden of implementing such aspect(s).

A. Section 160.103—Definitions

1. Current Provision

Electronic media are used by many health care organizations to process, transmit, and maintain ePHI. As defined by the Security Rule, the term ''electronic media'' [334] encompasses both (1) electronic storage material on which data is or may be electronically recorded; and (2) transmission media used to exchange information already in electronic storage media. It specifically excludes certain transmissions, such as those of paper, via facsimile (''fax''), and voice, via telephone, from being considered transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

2. Issues To Address

The Department revised the definition of ''electronic media'' in 2013 by replacing the term ''electronic storage media'' with ''electronic storage material'' in recognition that there may be storage material other than ''media'' that houses electronic data in the future.[335] At that time, the Department said that a fax machine accepting a hardcopy document for transmission is not a covered transmission even though the document may have originated from printing from an electronic file.[336] In response to commenter concerns, we also clarified that ePHI maintained, intentionally or otherwise, in a photocopier, fax machine, or other device is subject to the Security Rule and reminded regulated entities that they should be aware of the capabilities of such devices with respect to their ability to maintain ePHI.[337] Additionally, a regulated entity should consider the appropriateness of implementing security measures that account for such capabilities.[338]

Since 2013, the role technology plays in the storage and transmission of information has changed, as have the types of media used to store and transmit such information. For example, traditional landlines [339] are rapidly being replaced with electronic communication technologies, such as Voice over internet Protocol (VoIP),[340] and mobile technologies that use electronic media, such as the internet, intra- and extranets, cellular, and Wi-Fi.[341] Some current electronic technologies that regulated entities use for remote communications may include communication applications on a smartphone or another computing device, VoIP technologies, technologies that electronically record or transcribe a telehealth session, and messaging services that electronically store audio messages. The definition of electronic media does not account for these changes because it excepts

[334] 45 CFR 160.103 (definition of ''Electronic media'').

[335] 78 FR 5566 (Jan. 25, 2013).

[336] *Id.* at 5576.

[337] *Id.*

[338] *Id.*

[339] A standard telephone line, often described as a traditional landline, uses circuit-switched voice communication service technologies through the Public Switched Telephone Network. The information transmitted through such traditional telephones is not electronic.

[340] VoIP technologies convert audio into a digital signal that is then transmitted over the internet. *See* Voice Over internet Protocol (VoIP), Federal Communications Commission, *https://www.fcc.gov/general/voice-over-internet-protocol-voip.*

[341] A 2022 report by the Federal Communications Commission stated that the ''number of fixed retail switched-access lines declined over the past three years at a compound annual rate of 12.3%, while interconnected VoIP subscriptions increased at a compound annual growth rate of 0.7%.'' *See* ''2022 COMMUNICATIONS MARKETPLACE REPORT,'' Federal Communications Commission, p. 122 (Dec. 30, 2022), *https://docs.fcc.gov/public/attachments/FCC-22-103A1.pdf.*

transmissions via fax, and of voice, via telephone, from transmissions via electronic media, nor does the definition take into consideration new and emerging technologies. Accordingly, the Department believes that it is appropriate to reconsider this definition.

3. Proposals

The Department proposes to modify the definition of ''electronic media'' as follows. First, the Department proposes to revise paragraph (1) of the definition to clarify that electronic media includes not only media on which data may be recorded, but also media on which data may be maintained or processed.

Generally, data is either at rest, in transit, or in process (*e.g.,* being worked on, in use, being modified in memory, or being updated).[342] After the data is no longer in use, it is either maintained or transmitted. It is especially important for entities to protect data in process because generally, data must be unencrypted to be processed, making this a time when it is particularly vulnerable to a breach or other security incident.[343] To that end, the Department's proposal would clarify that the definition includes electronic media that is used to record, maintain, or process data.

The Department also proposes to revise paragraph (1) to clarify and update terminology used in a non-exhaustive list of examples of electronic storage material. Additionally, to ensure that the definition includes future technology, the Department proposes to add to the list of examples ''any other form of digital memory or storage'' on which data may be recorded, maintained, or processed.

As discussed above, traditional landlines and fax machines are rapidly being replaced with electronic communication technologies and mobile technologies that use electronic media. The Security Rule applies when a regulated entity uses such electronic communication technologies. Therefore, regulated entities using telephone systems and fax equipment that transmit ePHI need to apply the Security Rule safeguards to those technologies.[344] Accordingly, in paragraph (2), we propose to revise the description of ''transmission media'' to recognize that data is transmitted almost exclusively in electronic form today. The limited exception to this would be data that is handwritten on paper and hand-delivered or mailed, such that the data is never on electronic storage material. Additionally, the Department proposes to include public networks in the examples of transmission media and to remove the sentence that describes transmissions that are not considered transmissions via electronic media. By making these changes, we would reflect technology's evolution since 2013.

We also propose to make a technical correction to paragraph (2) of the definition, consistent with a revision made in the 2013 Omnibus Rule to paragraph (1).[345] Specifically, the Department proposes to replace the term ''electronic storage media'' with ''electronic storage material'' in paragraph (2) to clarify the connection between definitions of electronic storage material and transmission media. We neglected to make this change in 2013 when we replaced ''electronic storage media'' with ''electronic storage material'' in paragraph (1), which means that paragraph (2) relies on a term that is no longer defined. This technical correction we propose is consistent with how the Department has interpreted the definition of transmission media and the connection between it and electronic storage material since the change was made in 2013.

4. Request for Comment

The Department requests comment on the foregoing proposals, including any benefits, drawbacks, or unintended consequences. We also request comment on the following considerations in particular:

a. Whether the proposed modifications accurately capture current use of electronic media.

b. Whether the proposed modifications allow for future technological innovation.

c. Whether there are other types of electronic storage material that the Department should include in the non-exhaustive list of examples.

d. Whether there are other types of transmission media that the Department should include in the non-exhaustive list of examples.

B. Section 164.304—Definitions

Section 164.304 includes definitions for key regulatory terms in the Security Rule. The Department proposes to add ten new defined terms and to modify the definitions of fifteen existing terms. The proposed new regulatory terms would be: Deploy, Implement, Electronic information system, Multi-factor authentication, Relevant electronic information system, Risk, Technical controls, Technology asset, Threat, and Vulnerability. The definitions we propose to modify are for the following terms: Access, Administrative safeguards, Authentication, Availability, Confidentiality, Information system, Malicious software, Password, Physical safeguards, Security or Security measures, Security incident, Technical safeguards, User, and Workstation. Generally, the Department is proposing to add or modify regulatory terms that would either clarify how regulated entities should apply the standards and implementation specifications or modernize the rule to better account for changes in the environment in which health care is provided.

1. Clarifying the Definition of ''Access''

a. Current Provision and Issues To Address

The Security Rule defines the term ''access'' as the ability or means necessary to perform a set of activities describing how a user may interact with a system resource.[346] These activities are reading, writing, modifying, communicating data/information, or otherwise using any component of an information system. The definition applies only to the Security Rule, not to the Breach Notification Rule or the Privacy Rule.

The term ''access'' defines the scope of some key regulatory provisions in the Security Rule. For example, whether a person meets the definition of a ''user'' is determined based on whether their access to information or a component of the regulated entity's information system is authorized.[347] The definition

[342] *See* ''NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0,'' National Institute of Standards and Technology, U.S. Department of Commerce, p. 29 (Jan. 16, 2020) (see definition of ''data processing''), *https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.*

[343] *See* Maithilee Joshi, et al., ''Delegated Authorization Framework for EHR Services Using Attribute-Based Encryption,'' IEEE Transactions on Services Computing, Volume 14, No. 6, p. 1 (2021) (discussing that health care providers are increasingly using Cloud-based EHR services to manage ePHI, which increases the possibility of attacks on ePHI), *https://ebiquity.umbc.edu/get/a/publication/1126.pdf; see also* ''Security Standards: Technical Safeguards,'' HIPAA Security Series, Office for Civil Rights, U.S. Department of Health and Human Services, (May 2005, revised Mar. 2007) (The goal of encryption is to protect ePHI from being accessed and viewed by unauthorized users.), *https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf?language=es.*

[344] The Department previously acknowledged that information transmitted by a telephone voice response system in response to a telephone request, and some voice technology digitally produced from an information system and transmitted by telephone are both covered by this definition. See 68 FR 8334, 8342 (Feb. 20, 2003); 75 FR 40868, 40874 (July 14, 2010); and 78 FR 5566, 5575 (Jan. 25, 2013).

[345] 78 FR 5566, 5575–5576 (Jan. 25, 2013).

[346] 45 CFR 164.304 (definition of ''Access'').

[347] 45 CFR 164.304 (definition of ''User'').

of the term ''security incident'' requires consideration of whether a person attempted to access or accessed information without authorization.[348] To determine whether a regulated entity complied with the administrative safeguard standard for workforce security, the Department must consider to what extent a regulated entity established policies and procedures for ensuring that workforce members have appropriate access to ePHI.[349]

The current definition is expansive but not fully representative of how users could interact with information today. As discussed above, users create, receive, maintain, and transmit information in more ways now than they did ten years ago. Thus, the Department believes that it is critical for the Department to consider modifying the definition of this term to adequately reflect the current electronic environment.

b. Proposal

The Department proposes to expand the list of activities that should be considered under the term by adding the activities of ''deleting'' and ''transmitting.'' The Department also proposes to replace ''system resource'' with ''component of an information system'' to rely on an already defined term, ''information system.'' The proposed modification would clarify that the term includes any and all components of an information system and an information system as a whole. Additionally, the Department believes that a component of an information system better describes how the term access applies today because it is inclusive of hardware, software, and people, as opposed to only the inherent capabilities that contribute to performance, such as system memory and hard disk space.

2. Clarifying the Definition of ''Administrative Safeguards''

a. Current Provision and Issues To Address

Administrative safeguards are administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance (including reviewing and modifying) of security measures to protect ePHI.[350] Administrative safeguards also manage the conduct of the regulated entity's workforce in relation to the protection of ePHI. Under the Security Rule, there are minor inconsistencies in language between the definitions of the types of safeguards, which might lead to uncertainty about how to interpret the terms and lead to unintended consequences. For example, the definitions of ''administrative safeguards'' and ''physical safeguards'' use ''are,'' while the definition of technical safeguards uses ''means.'' [351]

In addition, the existing definition of ''administrative safeguards'' does not expressly relate the administrative actions to the policies and procedures addressing the activities covered by the definition, nor does it make clear that the policies and procedures are in addition to the administrative actions. The same is true for the definitions of physical and technical safeguards. Further, the definition of ''administrative safeguards'' does not expressly mention managing updates and modifications to safeguards.

b. Proposal

To address the minor inconsistencies between the definitions of the safeguards and to ensure that each safeguard is afforded an equal weight of importance, the Department proposes similar but minor changes across the definitions. The Department proposes to add the word ''related'' to the definition here, and below to add the words ''and related'' when necessary, to more clearly connect the components that make up safeguards. In the case of administrative safeguards, the Department's proposal relates administrative actions to administrative policies and procedures. The Department believes that this change would reduce confusion and improve clarity about compliance obligations. We are proposing a similar change to the definitions of physical safeguards and technical safeguards below. Additionally, we are proposing to clarify that maintenance includes updating and modifying with respect to administrative safeguards.

3. Clarifying the Definition of ''Authentication''

a. Current Provision and Issues To Address

The Security Rule defines authentication as corroboration that a person is the one claimed. By limiting the definition of authentication to persons, the current definition neglects to acknowledge the importance to the security of ePHI of authenticating technology assets that are components of a regulated entity's electronic information systems that create, receive, maintain, or transmit ePHI or that otherwise affect the confidentiality, integrity, or availability of ePHI, or that the regulated entity intends to connect to such electronic information systems.[352] Absent such authentication, a bad actor could add technology assets (*e.g.,* software) to a regulated entity's electronic information systems that enable the bad actor to compromise the security of ePHI.

b. Proposal

To modernize the definition of authentication to reflect best practices in cybersecurity today, the Department proposes to clarify the definition to mean corroboration that either a person or technology asset is the one they are claiming to be. The modified definition would also improve readability with minor changes in wording. The Department believes as proposed, the revised definition would more accurately reflect the role played by technology assets in electronic information systems today. For example, a covered health care provider permits individuals to access their own PHI using an application that connects to the software that runs the covered health care provider's patient portal. Not only must the individual be authenticated as a user, but the application must be authenticated such that the covered entity's software can verify that the application is what it claims to be. In another example, a portable technology asset for retrieving and storing PHI in the cloud must be authenticated before retrieving data from cloud storage.

4. Clarifying the Definition of ''Availability''

a. Current Provision and Issues To Address

''Availability'' is defined in the Security Rule as the property that data or information is accessible and usable upon demand by an authorized person. Although not intended, the current definition could be read to limit the scope of availability only to authorized persons. And yet, it is equally important to ensure that authorized technology assets, such as connected medical devices, software, and workstations,

[348] 45 CFR 164.304 (definition of ''Security incident'').

[349] 45 CFR 164.308(a)(3)(i); proposed 45 CFR 164.308(a)(9)(i).

[350] 45 CFR 164.304 (definition of ''Administrative safeguards'').

[351] 45 CFR 164.304 (definitions of ''Administrative safeguards,'' ''Physical safeguards,'' and ''Technical safeguards'').

[352] *See also* Special Publication 800–82r3, Guide to Operational Technology Security, National Institute of Standards and Technology, section 6.2.1, p. 97, Identity Management and Access Control (PR.AC) (discussing the need of organizations to apply authentication controls for users, devices, and processes within the technology environment) (September 2023).

have access on demand to ePHI to carry out their functions.

b. Proposal

Given the increased connectivity of the health care environment, the Department proposes to clarify the definition of availability by specifying that availability means the property that data or information is accessible and usable upon demand by not only an authorized person, but also an authorized technology asset. In so doing, the Department is not changing the meaning of availability, but rather clarifying its scope.

5. Clarifying the Definition of ''Confidentiality''

a. Current Provision and Issues To Address

Similar to the definition of availability, the definition of the term ''confidentiality'' could be read as limited to the property that data or information is not made available or disclosed to unauthorized persons or processes. Read that way, the definition does not reflect today's health care environment in which data and information may be accessed through any component of an interconnected electronic information system.

b. Proposal

The Department proposes to clarify the definition of confidentiality to specify that it means the property that data or information is not made available or disclosed to unauthorized persons, technology assets, or processes.

6. Adding Definitions of ''Deploy'' and ''Implement''

a. Issues To Address

The Security Rule directs regulated entities to implement technical policies and procedures and assumes that such implementation requires the installation and configuration of technical safeguards.[353] OCR is concerned, based on its investigations and compliance reviews, that some regulated entities may interpret the regulatory requirement to implement technical policies and procedures to mean that a regulated entity is only required to establish written policies and procedures about technical requirements, but need not then apply effective, automated technical policies and procedures to all ePHI throughout the regulated entity's enterprise. For example, in *M.D. Anderson,* the court stated that the encryption requirement at 45 CFR 164.312(a)(2)(iv) requiring a regulated entity to implement a mechanism to encrypt ePHI does not ''require a covered entity to warrant that its mechanism provides bulletproof protection of 'all systems containing ePHI.' Nor does it require covered entities to warrant that all ePHI is always and everywhere 'inaccessible to unauthorized users.' '' [354] Further, the court added that the requirement does not ''say anything about how effective a mechanism must be, how universally it must be enforced, or how impervious to human error or hacker malfeasance it must be.'' [355]

Therefore, the Department believes it is necessary to add definitions that distinguish between implementation of the administrative and technical safeguards by separately describing how regulated entities can comply with requirements to implement technical safeguards and install technical solutions.

b. Proposal

The Department proposes to define the term ''deploy'' to identify a specific type of ''implementation.'' We believe that the new term and definition would help to better describe the compliance obligations for implementation specifications related to the use of technology for securing the confidentiality, integrity, or availability of ePHI. As proposed, the definition would require a regulated entity to ensure that technology is in place, configured for use, and actually in use and operational throughout the regulated entity. The Department's proposed use of the term helps illustrate its purpose and utility in clarifying that policies and procedures, while necessary, are insufficient to meet requirements for technical safeguards.

For example, the Department is proposing to create a new requirement for regulated entities to verify that business associates have deployed technical safeguards—that is, the technology is configured and operational, not only addressed in policies and procedures.[356] In another example, the Department is proposing new implementation specifications under the access control standard that would require a regulated entity to deploy technical controls for relevant electronic information systems so that the system is configured and applied to limit access to only users and technology assets that have been granted access rights.[357] In the automatic logoff implementation specification for that same standard, the Department is proposing to replace the requirement to implement electronic procedures for terminating an electronic session with a requirement to deploy technical controls that terminate an electronic session after a period of inactivity.[358] In each case, the technical controls must not only be configured for use, but they also must be applied to and in effect in all ePHI and relevant electronic information systems.

The Department proposes to define the term ''implement'' to clarify that a safeguard must be put into place and be in effect throughout the enterprise, as opposed to only some components of a regulated entity's relevant information systems (*e.g.,* some laptops or servers) or applied to a subset of ePHI. The Department also proposes the term to further clarify what it means to configure and put technology, technical controls, and related policies and procedures into effect and be in use, operational, and function as expected throughout the regulated entity's enterprise (*i.e.,* deploy) as compared to putting into place and making effective administrative or physical safeguards. Further, the Department proposes to expressly clarify that implement also means that a safeguard must function as expected. Under this proposal, if adopted, we would not consider a safeguard to be implemented if it is not functioning in the manner in which it is expected.

For example, a regulated entity's administrative policy requiring it to take action to prevent infections from malicious software is not implemented until it is applied throughout the enterprise, meaning that the entity has ensured that anti-malware protections have been put into place on all relevant electronic information systems that create, receive, maintain, or transmit ePHI or that otherwise affect the confidentiality, integrity, or availability of ePHI throughout the enterprise.

Similarly, to operationalize such a policy, the regulated entity must deploy technology assets and/or technical controls to block such software according to its technical policies and

[353] While the Department also regulates ''adoption and meaningful use of certified EHR technology,'' such as the actions of the end-user with respect to having and meaningfully using certified health IT to meet certain requirements, such as those requirements for the Promoting Interoperability performance category of the Merit-based Incentive Payment System (MIPS) (sections 1848(q)(2)(B)(iv) and 1848(o)(2) of the SSA), the definitions proposed in this NPRM would apply only to regulated entities' compliance with the Security Rule.

[354] *University of Texas M.D. Anderson Cancer Center, supra* note 258, p. 478.

[355] *Id.*

[356] *See* proposed 45 CFR 164.308(b)(1)(i) and (ii) and (b)(2)(ii).

[357] *See* proposed 45 CFR 164.312(a)(1).

[358] *See* proposed 45 CFR 164.312(a)(2)(iv).

procedures. In this regard, the proposed term ''deploy'' clarifies that the technology assets or technical control must be put into place, configured, and actually work (*i.e.,* function in the manner expected of the technology or technical control) throughout a regulated entity, in addition to the relevant policy and procedures being applied across a regulated entity. To implement a policy and procedure is separate from the implementation of a technology asset or technical control but in both cases, the underlying requirement is application across the enterprise.

7. Adding a Definition of ''Electronic Information System''

a. Issues To Address

The current Security Rule includes explicit requirements for regulated entities to protect electronic information systems by implementing policies and procedures to limit physical access to such systems [359] and by implementing technical policies and procedures for electronic information systems that maintain ePHI to allow access to only persons or technology assets that have been granted access rights pursuant to 45 CFR 164.308(a)(4).[360] Further, the physical measures, policies, and procedures that meet the definition of physical safeguards are specifically limited to those that protect regulated entities' electronic information systems and related buildings and equipment.[361] And yet, the Security Rule does not explicitly define this term. Instead, it assumes that the definition is easily understood to be a subset of information system, a broad term that is not limited by the boundaries of the Security Rule. The Department believes that regulated entities would benefit from additional clarity regarding the definition of this term, given its foundational nature.

b. Proposal

The Department proposes to add a definition of ''electronic information system'' to better distinguish the concept from the broader category of an information system. Accordingly, the Department would limit the definition to an interconnected set of electronic information resources under the same direct management control that shares common functionality. Under this proposal, an electronic information system generally would include technology assets, such as hardware, software, electronic media, data, and information.

8. Modifying the Definition of ''Information System''

a. Current Provision and Issues To Address

As discussed above, the Department seeks to clarify the scope of an information system, as compared to an electronic information system. We believe that it would be beneficial to align the common elements of these terms and clarify the relationship between them, given their importance to compliance with requirements of the Security Rule. Additionally, the changes in the environment, such as the shift to cloud-based computing, may raise questions regarding the Department's interpretation of ''direct management control.''

b. Proposal

Accordingly, the Department proposes to modify the definition of ''information system,'' to clarify that an information system ''generally'', not just ''normally,'' includes hardware, software, data, communications, and people. The Department believes this proposed modification, combined with the existing broad reference to ''resources,'' more accurately reflects the typical components of an information system and the full extent of resources that are addressed by the Security Rule. We also propose to remove ''applications'' from the list of technology assets that are generally included in an information system because applications are a type of software, making the inclusion of applications redundant. This proposed modification would not alter our interpretation that an information system includes applications.

We use this opportunity to affirm that a technology asset may be included as part of the information systems of multiple regulated entities where such regulated entities all have direct management control over the technology asset. For example, both a health care provider and a cloud-based EHR vendor have direct management control over the ePHI in the cloud-based EHR. Accordingly, such ePHI generally is part of both the information system of the health care provider and of the cloud-based EHR vendor. Additionally, the EHR that is used to create, receive, maintain, or transmit ePHI, regardless of whether it is accessed using software installed on the health care provider's workstation(s) or an internet browser, generally is also part of the information system of both entities because both the health care provider and the vendor have direct management control over the EHR.

9. Modifying the Definition of ''Malicious software''

a. Current Provision and Issues To Address

Persons seeking unauthorized access to data and information are increasingly sophisticated. Their methods of attempting to gain such access can take many forms and result in a wide array of harms, as discussed above. One of the methods they use is through the introduction of malicious software (also referred to as malware) into an electronic information system. As the sophistication of bad actors has increased, so has the variety of types of malicious software that they use to access electronic information systems. The Security Rule defines malicious software but limits it to software designed to damage or disrupt a system. The regulatory text provides only one example of malicious software in regulatory text—a virus.

b. Proposal

The Department proposes to replace the current definition of malicious software with one that would be consistent with how cybersecurity experts define the term today.[362] Specifically, we propose to define it to mean software or firmware intended to perform an unauthorized action or activity that will have adverse impact on an electronic information system and/or the confidentiality, integrity, or availability of electronic protected health information. This proposal would therefore clarify that malicious software could include either software or firmware and that the negative effects of the malicious software may not be limited to damaging or disrupting a system. Rather, effects of the software could be intended to have any type of adverse impact on an electronic information system and/or the confidentiality, integrity, or availability of ePHI. The Department also proposes to include in regulatory text a non-exhaustive list of examples, such as viruses, worms, Trojan horses, spyware, and some forms of adware, to assist regulated entities in understanding what constitutes malicious software.

[359] *See* 45 CFR 164.310(a)(1).

[360] *See* 45 CFR 164.312(a)(1).

[361] 45 CFR 164.304 (definition of ''Physical safeguards'').

[362] *See* NIST definition of ''malware,'' Glossary, Computer Security Resource Center, National Institute for Standards and Technology, U.S. Department of Commerce, *https://csrc.nist.gov/glossary/term/malware.*

10. Adding a Definition of ''Multi-Factor Authentication'' (MFA)

a. Issues To Address

The Security Rule includes several technical safeguard provisions that require regulated entities to identify and authenticate persons accessing information and systems to protect ePHI. Section 164.312(a)(2)(1) includes the standard that requires a regulated entity to implement technical policies and procedures that limit access to ePHI to only those persons or software programs that have been granted access rights, while 45 CFR 164.312(d)(2), the standard for person or entity authentication, requires a regulated entity to implement procedures to verify that a person seeking access to ePHI is the one claimed.

Historically, regulated entities relied on combinations of usernames and passwords to identify users and authenticate users to the system. We recognize that such combinations are insufficient to secure sensitive information and that more sophisticated mechanisms for doing so have been developed. As a best practice for managing cyber threats, most cybersecurity frameworks, including those discussed above, recommend that organizations adopt solutions that rely on multiple factors to identify and authenticate users. For example, the HHS 405(d) Program's ''Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients'' [363] recommends a layered approach to cyber defense (*i.e.,* if a first layer is breached, a second exists to prevent a complete breach).[364] It further provides that MFA as a source of identity and access security control is an important means to control access to infrastructure and conduct proper change management control.[365] The Department's CPGs [366] identify MFA as an essential goal and a critical, additional layer of security for the protection of assets and accounts that are directly accessible from the internet.[367] The Department has also explained in guidance that weak authentication processes leave organizations vulnerable to intrusion, while effective authentication ensures that only authorized entities may access information systems and data.[368] Additionally, CISA has issued recommendations for implementing MFA, specifically MFA solutions that are phishing resistant to protect against disclosures of authentication data to a bad actor.[369]

b. Proposal

The Department proposes to define the term ''Multi-factor authentication'' to provide regulated entities with a specific level of authentication for accessing relevant electronic information systems.[370] Regulated entities would be required to apply this proposed definition when implementing the proposed rule's specific requirements for authenticating users' identities through verification of at least two of three categories of factors of information about the user. The proposed categories would be:

- Information known by the user, including but not limited to a password or personal identification number (PIN).
- Item possessed by the user, including but not limited to a token or a smart identification card.
- Personal characteristic of the user, including but not limited to fingerprint, facial recognition, gait, typing cadence, or other biometric or behavioral characteristics.

MFA relies on the user presenting at least two factors. Authentication that relies on multiple instances of the same factor, such as requiring a password and PIN, is not MFA because both factors are ''something you know.'' [371] For example, where MFA is deployed, users could seek access by entering a password. However, without the entry of at least a second factor such as a token [372] or smart identification card, the user is not granted access and the password is useless by itself. Cybercriminals seeking access to MFA-protected information systems require significantly more resources to launch the attack because there are multiple data points required to succeed.[373]

The Department proposes that the personal characteristics that could be used as factors would include both physical characteristics, such as fingerprints or facial identifiers, and behavioral characteristics, such as a user's gait or typing cadence.[374]

11. Clarifying the Definition of ''Password''

a. Current Provision and Issues To Address

The Security Rule currently defines ''password'' as confidential authentication information composed of a string of characters.[375] The definition provides no further regulatory instruction on what constitutes a ''character'' for purpose of compliance.

b. Proposal

The Department proposes to add examples to the definition to further clarify what constitutes a character, and adds ''such as letters, numbers, spaces, and other symbols'' to the existing definition. The Department believes that regulatory examples would provide necessary context for regulated entities that deploy safeguards involving passwords.

---

[363] ''Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients,'' *supra* note 16.

[364] *Id.* at 15.

[365] *Id.*

[366] ''Cybersecurity Performance Goals,'' *supra* note 18.

[367] *Id.*

[368] *See* ''HIPAA and Cybersecurity Authentication,'' Cybersecurity Newsletter, Office for Civil Rights, U.S. Department of Health and Human Services (June 2023), *https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-june-2023/index.html.*

[369] *Id.* (citing ''Implementing Phishing-Resistant MFA,'' Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security (Oct. 2022), *https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf*); NIST also has issued draft defined characteristics for phishing-resistant authenticators. *See* David Temoshok, et al., ''Digital Identity Guidelines,'' NIST Special Publication 800–63–4 2pd (Second Public Draft), National Institute of Standards and Technology, U.S. Department of Commerce, p. 36 (Aug. 21, 2024), *https://csrc.nist.gov/pubs/sp/800/63/4/2pd.*

[370] *See* proposed 45 CFR 164.312(f)(2)(ii).

[371] *See* ''HIPAA and Cybersecurity Authentication,'' *supra* note 368 (citing David Temoshok, et al., ''Digital Identity Guidelines,'' NIST Special Publication 800–63–4 (Initial Public Draft), National Institute of Standards and Technology, U.S. Department of Commerce, p. 17 (Dec. 2022), *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.ipd.pdf*).

[372] NIST defines ''token'' as ''a portable, user-controlled, physical device (*e.g.,* smart card or memory stick) used to store cryptographic information and possibly also perform cryptographic functions.'' *See* NIST definition of ''token,'' Glossary, Computer Security Resource Center, National Institute of Standards and Technology, U.S. Department of Commerce (citing Elaine Barker, et al., ''Recommendation for Key Management: Part 2—Best Practices for Key Management Organizations,'' NIST Special Publication 800–57, Part 2, Revision 1, National Institute of Standards and Technology, U.S. Department of Commerce (May 2019)), *https://csrc.nist.gov/glossary/term/token#:~:text=NIST%20SP%20800%2D63%2D3%20under%20Token,possibly%20also%20perform%20cryptographic%20functions.*

[373] Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123, p. 7.

[374] *See* ''Digital Identity Guidelines: Authentication and Lifecycle Management'', NIST Special Publication 800–63B, National Institute of Standard and Technology, section 5.3.3, Use of Biometrics, (Oct. 16, 2023), *https://pages.nist.gov/800-63-3/sp800-63b.html#sec5.* We recognize that some of the example characteristics may not satisfy today's standards; however, the Department anticipates that they may in the future and proposes that they be included as examples such that regulated entities will be permitted to use them when the relevant standards are updated to allow for such use.

[375] 45 CFR 164.304 (definition of ''Password'').

12. Clarifying the Definition of ''Physical Safeguards''

a. Current Provision and Issues To Address

''Physical safeguards'' encompass the physical measures, policies, and procedures that protect a regulated entity's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion. As discussed within the definition of administrative safeguards, the Department believes that it is necessary to reduce minor inconsistences in language between the definitions of the types of safeguards. Additionally, the definition of physical safeguards relies on an undefined term (''buildings''), despite the existence of a defined term (''facilities'') that has an equivalent meaning.

b. Proposal

The Department proposes to clarify that the policies and procedures referred to in the definition are those that specifically are related to physical measures, and to replace ''buildings'' with ''facilities'' because facility is a defined term under the Security Rule and has an equivalent meaning.[376] The Department intends and has always intended the physical safeguards to apply to any location where a regulated entity might possess ePHI, including the physical premises and interior and exterior of a building, and any location that might affect the confidentiality, integrity, or availability of ePHI. Additionally, given the mobility of technology today, including workstations that may access ePHI, we believe it would be more appropriate to use the term facility to make clear that the physical safeguards are to apply throughout the premises of the regulated entity. For the same reasons discussed above, we also propose to clarify that the physical safeguards serve to protect relevant electronic information systems, as we propose to define the term elsewhere in this NPRM, rather than all electronic information systems. Further, the Department proposes to better standardize the administrative, physical, and technical safeguard requirements by using defined terms where they exist.

13. Adding a Definition of ''Relevant Electronic Information System''

a. Issues To Address

The Security Rule requires a regulated entity to ensure the confidentiality, integrity, and availability of all of the ePHI it creates, receives, maintains, or transmits.[377] To protect the ePHI as required, a regulated entity must also protect the electronic information systems that create, receive, maintain, or transmit ePHI and the electronic information systems that otherwise affect the confidentiality, integrity, or availability of ePHI. The Department believes that regulated entities are not consistently protecting ePHI in a manner that is consistent with their Security Rule obligations and believes that it is necessary to clarify the scope of those obligations. We believe that creating a new defined term for the electronic information systems to which the Security Rule requirements apply will help achieve this goal by ensuring that regulated entities fully understand how their technology assets and the architecture of their electronic information systems affect the confidentiality, integrity, and availability of ePHI.

b. Proposal

The Department proposes to add and define the term ''relevant electronic information system'' to mean an electronic information system that creates, receives, maintains, or transmits ePHI or that otherwise affects the confidentiality, integrity, or availability of ePHI. We believe that distinguishing between a relevant electronic information system and an electronic information system, as proposed, would further clarify the scope of regulated entities' compliance obligations, including the obligation of regulated entities to understand the relationship between their various electronic information systems and the confidentiality, integrity, and availability of ePHI.

The Department believes it is important to clarify that the requirements of the Security Rule do not only apply to electronic information systems that create, receive, maintain, or transmit ePHI. After all, cybercriminals may be able to access ePHI by leveraging vulnerabilities in some electronic information systems that do not themselves create, receive, maintain, or transmit ePHI where such information systems are connected to or otherwise affect electronic information systems that do create, receive, maintain, or transmit ePHI. For example, while a payment processing system used in a covered entity's food and beverage outlets or gift shops may not create, receive, maintain, or transmit ePHI, it may affect the confidentiality, integrity, or availability of ePHI in certain circumstances, such as where such systems are connected to the same network as servers that contain ePHI.[378] Accordingly, we would interpret an electronic information system as otherwise affecting the confidentiality, integrity, or availability of ePHI if it is insufficiently segregated physically and electronically from an electronic information system that creates, receives, maintains, or transmits ePHI or one that otherwise affects the confidentiality, integrity, or availability of ePHI.

An electronic information system would also fit the category of ''otherwise affecting'' if it contains information that relates to an electronic information system that creates, receives, maintains, or transmits ePHI or to another electronic information system that otherwise affects the confidentiality, integrity, or availability of ePHI. For example, a compromised electronic information system used to provide administrative functions, such as user authentication or management of storage area network infrastructure, that does not contain ePHI may allow unauthorized access to ePHI (affecting the confidentiality of ePHI) or disruption of storage configuration data (affecting the integrity and availability of ePHI). An electronic information system that is not connected to a covered health care provider's EHR but that maintains user IDs and passwords for the EHR also may not create, receive, maintain, or transmit ePHI; however, the confidentiality, integrity, or availability of the ePHI in the EHR would be affected if an unauthorized person gained access to that electronic information system. And the same is true for an electronic information system that contains the decryption keys for a regulated entity's encryption algorithms. Thus, it is important that administrative, physical, and technical safeguards be implemented not only for electronic information systems that create, receive, maintain, or transmit ePHI, but also for electronic information systems that otherwise affect the confidentiality, integrity, or availability of ePHI.

[376] *See* 45 CFR 164.304 (definition of ''Facility'').

[377] 45 CFR 164.306.

[378] *See, e.g.,* Steve Alder, ''$8.9 Million Banner Health Data Breach Settlement Gets Final Approval,'' The HIPAA Journal (Apr. 27, 2020), *https://www.hipaajournal.com/8-9-million-banner-health-data-breach-settlement-gets-final-approval/* (describing a settlement to cover claims stemming from an attack on a health system's payment processing system used in the food and beverage outlets of its hospitals).

14. Adding a Definition of ''Risk''

a. Issues To Address

The Security Rule does not currently include a definition for the term ''risk.'' The Department considered defining it when it first promulgated the final rule in 2003, but declined to do so because it determined that the term was commonly understood.[379] However, the Department now believes that the lack of a definition may affect the clarity of some key requirements for regulated entities. Such requirements include conducting a risk analysis to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the regulated entity [380] and implementing security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the general rules at 45 CFR 164.306(a).[381]

One of the ways NIST defines the term is as ''a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.'' [382] This and other NIST definitions serve as helpful references for the Department when considering how to define the term within the rule.

b. Proposal

The Department proposes to define ''risk'' as the extent to which the confidentiality, integrity, or availability of ePHI is threatened by a potential circumstance or event. The Department believes that defining the term would clarify several existing and proposed provisions of the Security Rule, such as the factors regulated entities must consider when determining the security measures they will implement [383] and the importance and purpose of conducting the required risk analysis.[384]

15. Clarifying the Definitions of ''Security or Security Measures'' and ''Security Incident''

a. Current Provision and Issues To Address

The Security Rule defines ''security or security measures'' as encompassing all of the administrative, physical, and technical safeguards in an information system.[385] The definition implies that the safeguards must be part of the information system, as opposed to something that may be applied or done to a system to protect the confidentiality, integrity, and availability of ePHI.

The rule also defines ''security incident'' as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. The existing definition does not make clear that a security incident may result from two types of behaviors—those related to attempted or successful but unauthorized access, use, disclosure, modification, or destruction of information in an information system, and those that are related to the attempted or successful unauthorized interference with system operations in an information system. In other words, a security incident may directly touch upon information in a system or interfere with the operations of the system itself. The Department believes that it is necessary to clearly convey the distinct types of incidents to regulated entities to ensure that regulated entities implement and deploy safeguards that address both concerns.

b. Proposal

The Department proposes to modify the definition of ''security or security measures'' to clarify that security or security measures may not only exist in information systems but may also be applied to information systems.[386] This clarification would better reflect the multi-layered approach to cybersecurity recommended by experts to address the concerns facing regulated entities today. For example, a regulated entity may determine that it is necessary to apply access controls and encryption mechanisms through an external mechanism, such as added firewall technology,[387] that is applied to the system, rather than technical controls that are embedded within the system or components of the system. The Department believes that the proposed definition would provide a more complete instruction.

The Department proposes to reorganize the definition of ''security incident'' into two numbered paragraphs to delineate the two separate categories of security incidents. We also propose to clarify that in both instances, the definition applies when the described action affects an information system and regardless of whether an attempt to affect the information in the system or interfere with system operations is successful or not.

16. Adding Definitions of ''Technical Controls''

a. Issues To Address

Throughout the technical safeguards provisions in 45 CFR 164.312, the Department directs regulated entities to implement technical policies and procedures. The court in *M.D. Anderson* interpreted technical policies and procedures as written policies and procedures on technical matters.[388] This interpretation does not reflect the Department's intent for technical safeguards to include policies and procedures that rely on technology or technological solutions for implementation.[389] We believe that the court's interpretation could have significant consequences for the confidentiality, integrity, and availability of ePHI.

b. Proposal

The Department proposes to add and define the term ''technical controls'' to help regulated entities better understand what we mean by technical safeguards for purposes of complying with the Security Rule. We propose to define technical controls as technical mechanisms contained in the hardware, software, or firmware components of an electronic information system that are primarily implemented and executed by the electronic information system to protect it and the data within the electronic information system. The Department believes that adding this term would better convey the expectation that a regulated entity is

[379] 63 FR 8334, 8340 (Feb. 20, 2003).

[380] 45 CFR 164.308(a)(1)(i)(A).

[381] 45 CFR 164.308(a)(1)(i)(B). Section 164.306(a) requires regulated entities to comply with four general requirements to protect ePHI.

[382] *See* NIST definition of ''risk,'' Glossary, Computer Security Resource Center, National Institute of Standards and Technology, U.S. Department of Commerce (citing William Newhouse, et al., ''Multifactor Authentication for E-Commerce,'' NIST Special Publication 1800–17, National Institute of Standards and Technology, U.S. Department of Commerce (July 2019)), *https://csrc.nist.gov/glossary/term/risk.*

[383] 45 CFR 164.304(b)(2)(iv).

[384] 45 CFR 164.308(a)(1)(ii)(A); proposed 45 CFR 164.308(a)(2)(i).

[385] 45 CFR 164.304 (definition of ''Security or Security measures'').

[386] 45 CFR 164.304 (definition of ''Security or Security measures'').

[387] *See* NIST definition of ''firewall,'' Glossary, Computer Security Resource Center, National Institute of Standards and Technology, U.S. Department of Commerce, *https://csrc.nist.gov/glossary/term/firewall.*

[388] *See generally University of Texas M.D. Anderson Cancer Center, supra* note 258, p. 478.

[389] For example, in the 2003 Final Rule, we explained that in developing technical safeguards, the Department proposed technical security services requirements and specific technical security mechanisms with implementation specifications without carving out or limiting these items to policies and procedures about the requirements. *See* 68 FR 8334, 8354 (Feb. 20, 2003).

required to deploy technical safeguards across its enterprise by, among other things, configuring and using technical mechanisms in the hardware, software, and firmware components of its relevant electronic information systems to protect ePHI and electronic information systems that create, receive, maintain, or transmit ePHI or that otherwise affect the confidentiality, availability, or integrity of ePHI.

17. Modifying the Definition of ''Technical Safeguards''

a. Current Provision and Issues To Address

The current definition of ''technical safeguards'' includes the technology and policy and procedures for its use that protect ePHI and control access to it.[390] As discussed above, the Department believes that there is an immediate need to modernize and update the definition to better reflect the role technology plays in protecting ePHI and the technical components of information systems, versus the role of policies and procedures. This would complement our effort to clarify the relationship between technology and the implementation of technical policies and procedures.

b. Proposal

The Department proposes to modify the definition of ''technical safeguards'' to expressly include ''technical controls.'' We also propose to add language that would clarify that the technology, technical controls, and related policies and procedures in this category govern the use of the technology to protect and control access to ePHI. The proposed changes also would improve the consistency of language across the safeguard provisions and rule.

18. Adding a Definition of ''Technology Asset''

a. Issues To Address

Throughout the Security Rule, standards and implementation specifications list the components of electronic information systems to which its requirements apply. Based on the Department's enforcement experience, we believe that it would be beneficial to more clearly distinguish between the requirements that apply to all components of an electronic information system and those that only apply to certain components. Additionally, we believe it would be beneficial to distinguish between requirements that apply specifically to each particular component of an electronic information system and those that apply to the electronic information system as a whole.

b. Proposal

The Department proposes to define the term ''technology asset'' to mean the components of an electronic information system, including but not limited to hardware, software, electronic media, information, and data. In so doing, we would clarify which Security Rule requirements apply to all of the components of electronic information systems as opposed to those that apply only to certain components, and which requirements apply to each particular components and which apply to the entire electronic information system.

For example, understanding the risks and vulnerabilities to a regulated entity's ePHI requires a thorough understanding of the components of its electronic information systems, the electronic information systems themselves, how they are connected, and how ePHI moves through those systems. Thus, by requiring a regulated entity to conduct an inventory of its technology assets and to create a network map of its electronic information systems, we clarify that a regulated entity is obligated to consider not only its electronic information systems as a whole, but also the components within those electronic information systems and their functions.

19. Adding a Definition of ''Threat''

a. Issues To Address

Addressing threats to the confidentiality, integrity, and availability of ePHI is a key function of the Security Rule, but the rule does not define ''threat.'' The concept of threat also underlies the Department's proposed definition of ''risk'' defined above and forms the basis of a key proposed implementation specification associated with the standard for risk analysis.[391]

b. Proposal

The Department proposes to define the term ''threat'' to mean any circumstance or event with the potential to adversely affect the confidentiality, integrity, or availability of ePHI. This proposal is similar to NIST's varying definitions of threat, edited to apply specifically to health care and the type of information addressed by the Security Rule.[392] Under this proposal, we would construe the term to apply broadly to include threats caused by, or existing because of, a variety of circumstances that specifically could affect the security of ePHI. Hackers, malicious insiders, and malicious software are examples of threat sources.

20. Clarifying the Definition of ''User''

a. Current Provision and Issues To Address

The Department first defined the term ''person'' in the HIPAA Rules as part of the 2003 ''Civil Money Penalties: Procedures for Investigations, Imposition of Penalties, and Hearings'' interim final rule to distinguish a ''natural person'' who could testify in the context of administrative proceedings from an ''entity'' (defined therein as a ''legal person'') on whose behalf a person would testify.[393] Although they were both published in 2003, the interim final rule was published two months after the Security Rule. Thus, when the Security Rule was published in 2003, it was necessary to specify that the term ''user'' included both natural persons and entities, but we believe that this is no longer the case because the current definition of ''person'' includes natural persons as well as entities.[394]

b. Proposal

The Department proposes to clarify the definition of ''User'' by removing the reference to an entity.[395] Because the definition of ''person'' includes an entity, including entity in the definition of ''user'' is redundant and could cause confusion. We believe that this is a technical correction because it would not change how the Department has interpreted the term.

21. Adding a Definition of ''Vulnerability''

a. Issues To Address

The term ''vulnerability'' is currently not defined in the Security Rule.

The Department previously explained that although some cyberattacks may be sophisticated and exploit previously unknown vulnerabilities (*i.e.,* zero-day attacks), most can be prevented or mitigated by addressing known vulnerabilities.[396] For example,

[390] 45 CFR 164.304 (definition of ''Technical safeguards'').

[391] Proposed 45 CFR164.308(a)(2)(ii)(A)(*2*).

[392] *See* NIST definition of ''threat,'' Glossary, Computer Security Resource Center, National Institute of Standards and Technology, U.S. Department of Commerce, *https://csrc.nist.gov/glossary/term/threat.*

[393] *See* 45 CFR 160.502 of the 2003 interim final rule, 68 FR 18895, 18898 (Apr. 17, 2003).

[394] 45 CFR 160.103 (definition of ''Person'').

[395] 45 CFR 164.304 (definition of ''User'').

[396] *See* ''Defending Against Common Cyber-Attacks,'' Cybersecurity Newsletter, Office for Civil Rights, U.S. Department of Health and Human

Continued

exploitable vulnerabilities exist across many components of IT infrastructures including, but not limited to, servers, desktops, mobile device operating systems, web software, and firewalls.[397] To mitigate against intrusions and hacking threats, the Department has recommended that regulated entities install vendor patches, make software updates, and monitor sources of cybersecurity alerts describing new vulnerabilities, such as the NIST National Vulnerability Database [398] and CISA's Known Exploited Vulnerabilities Catalog.[399]

b. Proposal

The Department proposes to define vulnerability by adopting substantially the same definition as NIST (a ''weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source'') [400] with minor changes to clarify how it applies to regulated entities and ePHI. The definition, if adopted as proposed, would then form the basis for understanding key assessment and mitigation strategies proposed in this NPRM, such as risk analyses,[401] patch management,[402] and vulnerability management and scans.[403]

22. Clarifying the Definition of ''Workstation''

a. Current Provision and Issues To Address

The Department currently defines the term ''workstation'' to mean an electronic computing device and provides the examples of technology that dominated the health care environment in 2003 and 2013, such as a laptop, desktop computer, and other device that performs similar functions, and electronic media stored in its immediate environment.[404] Workstations are essential for workforce members to perform their assigned functions, such as clinicians entering an individual's health history and treatment plan or billing staff preparing claims. Workstations are one of the key entry points for users to access a regulated entity's information systems. Thus, the Security Rule contains provisions requiring that regulated entities secure not only their information systems, but also individual workstations.[405] However, as discussed above, the health care environment has changed. It now includes both the physical and virtual environment and is replete with mobile devices and other types of devices that may serve as multi-functional workstations. Clinicians and other workforce members often rely on smart phones, smart watches, tablets, laptops, and even personal digital assistants, among other devices. These devices have proliferated, and so has their ability to perform a wide variety of functions with increasing sophistication. The Department believes that it is necessary to update the definition to reflect the evolved nature of the landscape.

b. Proposal

In recognition of this changed environment, the Department proposes to modify the definition of workstation to provide additional examples of what constitutes a workstation. Specifically, we propose to add the examples of a server, virtual device, and a mobile device such as a smart phone or tablet. Virtual devices could include a virtual medical device, virtual server, or virtual desktop computer. The proposed definition also would clarify that technology properly considered as a ''workstation'' is not limited to the proposed regulatory examples.

23. Request for Comment

The Department requests comment on all the foregoing proposed definitions, including any benefits, drawbacks, or unintended consequences. We also request comment on the following considerations in particular:

a. Whether any of the proposed definitions would be problematic for regulated entities or result in unintended adverse consequences. If so, please explain.

b. Whether the Department should consider an alternative definition for any terms the Department proposes to define in the rule. If the answer is yes, please propose such an alternative definition and a reference or supporting rationale.

c. Whether the Department should define any additional terms within the rule. If the answer is yes, please propose such additional terms and definitions, along with any reference or supporting rationale.

d. With respect to the definitions of ''information system'' and ''electronic information system,'' the extent of a covered entity's direct management control over applications in cloud computing environments, such as a cloud-based EHR system.

e. With respect to the definitions of ''information system'' and ''electronic information system,'' the extent of a business associate's direct management control over applications in cloud computing environments, where the business associate is the cloud service provider.

f. Whether defining the term ''technical controls'' and adding it to the definition of ''technical safeguards'' would more clearly explain the requirements of 45 CFR 164.312.

g. Whether defining ''implement'' and ''deploy'' as we propose would more clearly explain the differences between what is expected of regulated entities with respect to administrative and physical safeguards and technical safeguards. To the extent that the proposals would not clarify the differences, please provide alternative solutions.

C. Section 164.306—Security Standards: General Rules

1. Current Provisions

Section 164.306 applies to regulated entities and includes the general rules for security standards. Generally, paragraph (a) codifies HIPAA statutory requirements for safeguarding ePHI.[406] Under these rules, regulated entities are required to do all of the following:

- Ensure the confidentiality, integrity, and availability of all ePHI the regulated entity creates, receives, maintains, or transmits.[407]
- Protect against reasonably anticipated threats or hazards to the security or integrity of such information.[408]
- Protect against any reasonably anticipated uses or disclosures of such information not permitted by the Privacy Rule.[409]
- Ensure that workforce members comply with the Security Rule.[410]

Paragraph (b) of this section permits regulated entities to determine the most

Services (Mar. 2022), *https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-first-quarter-2022/index.html.*

[397] *Id.*

[398] *Id.;* The National Vulnerability Database is the U.S. government repository of standards-based vulnerability management data. *See* ''National Vulnerability Database,'' National Institute of Standards and Technology, U.S. Department of Commerce, *https://nvd.nist.gov.*

[399] ''Known Exploited Vulnerabilities Catalog,'' Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security, *https://www.cisa.gov/known-exploited-vulnerabilities-catalog.*

[400] *See* NIST definition of ''vulnerability,'' Glossary, Computer Security Resource Center, National Institute of Standards and Technology, U.S. Department of Commerce, *https://csrc.nist.gov/glossary/term/vulnerability.*

[401] Proposed 45 CFR 164.308(a)(2)(ii)(A)(*7*).

[402] Proposed 45 CFR 164.308(a)(4)(i).

[403] Proposed 45 CFR 164.312(h)(1).

[404] 45 CFR 164.304 (definition of ''Workstation'').

[405] *See, e.g.,* 45 CFR 164.310(b) and (c).

[406] *See* 42 U.S.C. 1320d–2(d).

[407] *See* 42 U.S.C. 1320d–2(d)(2)(A).

[408] See 42 U.S.C. 1320d–2(d)(2)(B)(i).

[409] *See* 42 U.S.C. 1320d–2(d)(2)(B)(ii).

[410] *See* 42 U.S.C. 1320d–2(d)(2)(C).

appropriate security measures for protecting ePHI and their information systems. Accordingly, 45 CFR 164.306(b)(1) permits regulated entities to use any security measures to reasonably and appropriately implement the standards and implementation specifications of the Security Rule, while 45 CFR 164.306(b)(2) contains the factors that regulated entities are to consider when deciding which security measures to use. This paragraph furthers the aim of HIPAA's requirement for the security standards to take into account certain factors by providing for their consideration by regulated entities.[411] Accordingly, 45 CFR 164.306(b)(2) directs regulated entities to take these factors into account when determining the manner in which they will comply with the security standards and implementation specifications.

Section 164.306(c) requires regulated entities to comply with the administrative, physical, and technical safeguard standards in sections 45 CFR 164.308, 164.310, and 164.312 respectively, and with standards for organizational requirements and policies, procedures, and documentation requirements in sections 45 CFR 164.314 and 164.316. This provision is followed by paragraph (d), which explains that regulated entities are required to implement a specific implementation specification if described as ''required.'' If the implementation specification is described as ''addressable,'' regulated entities are required to implement the implementation specification if it is reasonable and appropriate to do so; or, if it is not reasonable and appropriate, document why and implement an equivalent alternative measure.

Finally, the maintenance provision at 45 CFR 164.306(e) requires regulated entities to review and modify security measures implemented under the Security Rule as needed to continue providing reasonable and appropriate protection of ePHI. It also requires regulated entities to update documentation of such security measures in accordance with the requirements for documentation at 45 CFR 164.316(b)(2)(iii).

2. Issues To Address

We believe that we can improve consistency in language between this section and other Security Rule provisions and better align this section with statutory terms and intent. For example, we are concerned that regulated entities are misinterpreting 45 CFR 164.306(a) to apply the requirements of the Security Rule to only some ePHI, rather than all ePHI. This interpretation could lead to inadequate protection of ePHI and relevant electronic information systems.[412] We also believe that consistency in language facilitates clear understanding and less ambiguity about how regulated entities must apply Security Rule standards.

Flexibility and scalability are among the Security Rule's defining characteristics, and we intend to preserve those elements to the extent possible. However, we believe that in this era of increased reliance on technology, more sophisticated cyber capabilities, and increasing cyberattacks, it is critical for regulated entities to implement and deploy strong security measures to protect ePHI and related information systems. We are concerned that regulated entities have focused their attention primarily on the cost of security measures, rather than considering the reasonableness and appropriateness of security measures in the context of all of the listed factors, including the probability and criticality of potential risks to ePHI.[413] Further, the Department believes that providing additional clarity would improve the ability of regulated entities to evaluate security measures for the protection of ePHI and the ability of a security measure to facilitate a regulated entity's recovery from emergencies and to support continued operations. With these proposed modifications, the Department seeks to ensure that regulated entities' reliance on the Security Rule's flexibility and scalability does not come at the expense of adequate security. The current regulation's framework in 45 CFR 164.306(b) lacks any express factor that would require an evaluation of the effectiveness of the security measures in supporting the resiliency of the regulated entity.

The Department has explained in regulation and guidance the difference between required and addressable implementation specifications. The meaning of ''required'' is clear. Regarding ''addressable,'' we previously explained that its purpose is to provide regulated entities flexibility with respect to implementation compliance.[414] We also previously explained that a regulated entity must assess whether a given addressable implementation specification is a reasonable and appropriate security measure to apply within its environment, and if it is, the regulated entity must implement the addressable implementation specification.[415] However, the Department remains concerned that regulated entities believe that flexibility overrides the need for them to protect all ePHI and do not uniformly treat addressable implementation specifications as needing to be met if they are reasonable and appropriate. OCR's enforcement experience and interaction with regulated entities causes us to believe that ''addressable'' is misunderstood to be optional, leading regulated entities to choose not to adopt the implementation specification, even when it would be reasonable and appropriate for them to do so.[416]

In 2022, NCVHS recommended that the Department eliminate the choice to not implement a specification or alternative, and instead require that regulated entities implement the specification or adopt a documented reasonable alternative.[417] According to a survey referenced by NCVHS, despite private sector and government efforts to address a changing cybersecurity landscape, the majority of health care entities have failed to maintain a comprehensive security program and

[411] The factors are: (1) the technical capabilities of records systems used to maintain health information; (2) the costs of security measures; (3) the need for training; (4) the value of audit trails in computerized record systems; and (5) the needs and capabilities of small and rural health care providers. *See* 42 U.S.C. 1320d–2(d)(1)(A)(i)–(v).

[412] *See University of Texas M.D. Anderson Cancer Center, supra* note 258, p. 478.

[413] 68 FR 8334, 8343 (Feb. 20, 2023).

[414] *See* ''What is the difference between addressable and required implementation specifications in the Security Rule?,'' Office for Civil Rights, U.S. Department of Health and Human Services, HIPAA FAQ #2020 (Dec. 28, 2022), *https://www.hhs.gov/hipaa/for-professionals/faq/2020/what-is-the-difference-between-addressable-and-required-implementation-specifications/index.html.*

[415] *See* 45 CFR 164.306(d)(3); ''What is the difference between addressable and required implementation specifications in the Security Rule?,'' *supra* note 414.

[416] The Department has consistently attempted to dispel the notion that addressable implementation specifications are optional. *See, e.g.,* ''Security 101 for Covered Entities,'' HIPAA Security Series, Centers for Medicare & Medicaid Services, p. 6 (Nov. 2004, revised Mar. 2007), *https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf?language=es;* ''*Controlling Access to ePHI: For Whose Eyes Only?,*'' *Cybersecurity Newsletter,* Office for Civil Rights, U.S. Department of Health and Human Services (July 14, 2021), *https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-summer-2021/index.html; and* ''*HIPAA Security Rule Facility Access Controls—What are they and how do you implement them?,*'' *Cybersecurity Newsletter,* Office for Civil Rights, U.S. Department of Health and Human Services (*Aug. 2024), https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-august-2024/index.html.*

[417] Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123, p. 2.

continue to neglect people and process measures necessary for a comprehensive security program.[418] NCVHS also pointed to a continued failure of regulated entities to develop adequate incident recovery plans and to assess their vulnerability to cyberattacks grounded in social engineering.[419] Finally, NCVHS opined that the current structure of the Security Rule is inadequate to protect U.S. health care infrastructure because it does not require regulated entities ''to adopt the basic building blocks of good security hygiene, or a documented, reasonable alternative.'' [420]

We share NCVHS' concerns and believe that we must squarely confront the problem of regulated entities treating addressable implementation specifications as optional. Relatedly, we also believe that we must consider modifying the Security Rule to set an acceptable minimum level of security specifications. Circumstances have changed sufficiently since 2003 such that we now believe that good cyber hygiene requires regulated entities to implement more than the implementation specifications that we originally mandated.[421] Indeed, we believe that it requires compliance with all of the standards and implementation specifications we are proposing, with specific, limited exceptions.

We also believe that the current maintenance requirement in 45 CFR 164.306(e) would benefit from increased specificity in light of the dramatic transformation of the health IT environment discussed above. For example, providing the frequency with which regulated entities must review and update their security measures would improve the security of ePHI and regulated entities' compliance with the Security Rule. The Security Rule's maintenance requirement would be further strengthened by requiring regulated entities to test their security measures to verify their sufficiency, and by clarifying the Department's expectations regarding documentation. Regulated entities' lack of documentation about how they implement security measures makes it difficult for them to know what security measures they have in fact implemented and to demonstrate compliance with the requirements of the Security Rule. Finally, the maintenance requirement in 45 CFR 164.306(e) is not included in or designated as a Security Rule standard, although it explicitly references the overarching documentation requirements in 45 CFR 164.316(b)(2)(iii). Thus, there is overlap between the two sections that may be causing confusion regarding the obligations of regulated entities to maintain security measures.

3. Proposals

a. Section 164.306(a)—General Requirements

The Department proposes to expand the introductory language to the general requirements provision at 45 CFR 164.306(a) to clarify the extent to which the general requirements apply to the obligations of regulated entities with respect to ePHI that they create, receive, maintain, or transmit.

Under the proposal, the Department would clarify that the general requirements apply to ''all'' ePHI. Additionally, the Department proposes to move language from paragraph (a)(1) to paragraph (a) to further emphasize that regulated entities must apply the requirements of the Security Rule to protect all of the ePHI they create, receive, maintain, or transmit. We also propose to clarify that ''each'' regulated entity would be required to apply the obligations in paragraphs (a)(1) through (4) to all ePHI it creates, receives, maintains, or transmits. The Department believes that this proposal would stress to regulated entities that each and every covered entity and business associate would be responsible for ensuring it meets Security Rule requirements with respect to all ePHI.

The Department believes this proposed change would also help address issues raised by current interpretations of the Security Rule that suggest that its plain wording may not require regulated entities to fully implement each security measure to protect all ePHI. Thus, the Department's proposed language would clarify that a security measure must be implemented such that it protects the security of all ePHI and all information systems that affect the confidentiality, integrity, and availability of ePHI.

Additionally, the Department proposes to modify the general requirements of paragraph (a)(2) to require each regulated entity to protect against any reasonably anticipated threats or hazards to the confidentiality, integrity, or availability of all ePHI, instead of to the security or integrity of ePHI. We believe that this proposal would better align this requirement with the general requirement at 45 CFR 164.306(a)(1), and confidentiality, integrity, and availability are generally considered the three basic elements of security.[422]

Additionally, the Department proposes a minor change to paragraph (a)(3) to refer specifically to ePHI, rather than using a more general term. We believe that both proposals would constitute technical revisions and that neither would alter the meaning of 45 CFR 164.306(a)(2) or (3), respectively.

Finally, the Department proposes to modify paragraph (a)(4) so that each regulated entity would be required to ensure that its workforce complies not only with the Security Rule, but also all administrative, physical, and technical safeguards implemented in accordance with this subpart.

These proposals would better align the language of the general requirements in paragraph (a) of 45 CFR 164.306 with the statute [423] and 45 CFR 164.530(c).[424] These proposals are also consistent with our proposals to revise the introductory language for each of the safeguard provisions to clarify the provisions therein would be the minimum regulated entities are to implement, *i.e.,* that the security measures required by the Security Rule constitute a floor of protections, not a ceiling.

b. Section 164.306(b)—Flexibility of Approach

The Department's proposals generally retain the flexible approach described in paragraph (b). As discussed above, the Security Rule carefully balances the benefits of safeguarding against risks to security and the burdens of implementing protective measures by, for example, enabling regulated entities to take into account specified factors when determining how to implement security measures in a manner that complies with the Security Rule. To acknowledge the rapid evolution of technology and increasing threats, the Department proposes to clarify

[418] *Id.* at Appendix p. 4.

[419] *Id.*

[420] *Id* at 5.

[421] *See* 68 FR 8334, 8336 (Feb. 20, 2003).

[422] 68 FR 8334, 8341 (Feb. 20, 2003); *see also* Jennifer Cawthra, et al., ''Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events,'' NIST Special Publication 1800–25A, National Institute of Standards and Technology, U.S. Department of Commerce, p. 1 (Dec. 2020) (''The CIA triad represents the three pillars of information security: confidentiality, integrity, and availability.''), *https://www.nccoe.nist.gov/publication/1800-25/VolA/index.html.*

[423] 42 U.S.C. 1320d–2(d)(2)(A) and (C).

[424] Section 164.530(c) includes the Privacy Rule standard and implementation specification for safeguarding PHI. It requires covered entities to have in place appropriate administrative, physical, and technical safeguards to protect the privacy of PHI. Additionally, it requires covered entities to reasonably safeguard PHI from intentional or unintentional uses or disclosures that violate the Privacy Rule, and to limit incidental uses or disclosures made pursuant to a permissible or required use or disclosure of PHI.

paragraph (b)(1) to provide that regulated entities are to apply reasonable and appropriate security measures to implement the standards and implementation specifications of the Security Rule. This proposal, if adopted, would replace the existing paragraph providing for regulated entities' reasonable and appropriate implementation of standards and implementation specifications, which could be misinterpreted to mean that a regulated entity may determine that implementation itself is unreasonable or inappropriate in some circumstances. That has never been the case. Thus, the proposed modification would clarify that implementation is not optional based on whether a regulated entity believes it is reasonable and appropriate; to the contrary, a regulated entity is required to implement the standards and implementation specifications and must adopt reasonable and appropriate security measures that allow the entity to achieve such implementation. The proposed clarification would comport more precisely with the statute, which requires regulated entities to maintain ''reasonable and appropriate'' safeguards.[425]

The Department also proposes to add a new element to the list of factors that regulated entities must take into account when deciding whether a particular security measure (*e.g.,* a technical control) is reasonable and appropriate for implementing a standard and its associated implementation specifications: the effectiveness of the security measure in supporting the resiliency of the regulated entity. A regulated entity would be required to consider this factor, in addition to the existing factors, for example, when choosing a specific encryption solution that allows the entity to meet the proposed requirement to encrypt ePHI, which will help prevent an unauthorized user from accessing the entity's ePHI; or when developing its security incident plan or disaster recovery plan, which will help ensure that the regulated entity can recover data or reestablish data integrity after a security incident or disaster.

The Department proposes at 45 CFR 164.306(b)(2)(v) to require a regulated entity to take into account how effectively its application of a particular security measure to achieve compliance with a standard and its associated implementation specifications would support its resiliency in the face of an event that adversely affects the entity. According to NIST, ''information system resilience'' addresses how well information systems ''continue to (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.'' [426] Recently, in this era of rising cybercrime, NIST described ''cyber resiliency'' as ''the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.'' [427] Thus, the Department proposes to require a regulated entity to consider the ability of its implementation of a particular security measure to aid it in preventing, withstanding, and recovering from an emergency or other occurrence that affects the confidentiality, integrity, or availability of ePHI, including a successful security incident.

The Department proposes this new requirement to better enable regulated entities to ensure the confidentiality, integrity, and availability of all ePHI that they create, receive, maintain, or transmit. The general rules require regulated entities to not only prevent threats and hazards to the confidentiality and integrity of ePHI, but also to ensure the availability of ePHI, even during a security incident that has the potential to severely hinder the ability of a regulated entity to provide health care or to bring it to a standstill. This new factor would require a regulated entity to consider whether a particular approach to complying with a standard and the associated implementation specifications can help it recover from an emergency or other occurrence, in addition to maintaining operations throughout the event. The Department proposes this factor to complement its proposals to strengthen the standards for security incident procedures [428] and contingency planning [429] and proposals for new standards for patch management [430] and vulnerability management,[431] discussed in detail below. If finalized, these proposals would help to ensure that regulated entities put in place the necessary measures to implement these standards.

The factors contemplate that regulated entities will regularly evaluate the security measures they have applied to comply with the standards and implementation specifications based on the technology available and known risks and vulnerabilities at the time of the evaluation. The Department expects that when the existing factors are considered with the factor proposed in this NPRM, a regulated entity would be required to consider whether a specific technical control has become sufficiently ubiquitous such that choosing not to adopt it would be unreasonable.

c. Section 164.306(c)—Standards and Implementation Specifications

To address the Department's concerns regarding the apparent misunderstanding by regulated entities of ''addressable,'' we propose to modify 45 CFR 164.306(c) and (d) by collapsing the separate paragraphs into one paragraph (c) to address both standards and implementation specifications and to remove the distinction between ''addressable'' and ''required'' implementation specifications. Instead, proposed paragraph (c), if adopted, would require regulated entities to comply with both the standards and implementation specifications. The Department believes that eliminating the distinction would make clear to regulated entities what has always been a requirement—that the Security Rule sets a floor for cybersecurity protections and that its flexibility is in allowing them to choose the manner in which they meet the standards and implementation specifications, not whether they meet them. The proposed change also would be consistent with NCVHS' recommendation to require regulated entities to meet certain minimum cybersecurity hygiene requirements.[432]

The Department acknowledges that proposing to remove the addressability distinction is a change from the approach adopted in the 2003 Final Rule. At that time, we explained that the decision to include addressable implementation specifications was made to provide additional flexibility to

[425] 42 U.S.C. 1320d–2(d).

[426] Joint Task Force, ''Managing Information Security Risk: Organization, Mission, and Information System View,'' NIST Special Publication 800–39, Appendix B, National Institute of Standards and Technology, U.S. Department of Commerce, p. B–5 (Mar. 2011), *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf.*

[427] Ron Ross, et al., ''Developing Cyber-Resilient Systems: A Systems Security Engineering Approach,'' NIST Special Publication 800–160, Volume 2, Revision 1, National Institute of Standards and Technology, U.S. Department of Commerce, p. 1 (Dec. 2021), *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf.*

[428] Proposed 45 CFR 164.308(a)(12)(i).

[429] Proposed 45 CFR 164.308(a)(13)(i).

[430] Proposed 45 CFR 164.308(a)(4)(i).

[431] Proposed 45 CFR 164.312(h)(1).

[432] *See* Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123, p. 5–10.

covered entities.[433] In this rulemaking, the Department proposes to strengthen protections and address evolving cybersecurity threats. While we acknowledge that this proposal would reduce the Security Rule's flexibility, we believe that it is necessary to do so to achieve HIPAA's purpose of an efficient and effective health care system that relies on the secure electronic exchange of ePHI. Importantly, removing the distinction between required and addressable would not eliminate all of the Security Rule's flexibility and scalability. Instead, it would simply clarify for regulated entities where the floor of protection must lie, and regulated entities must implement solutions that meet that floor, taking into consideration their needs and capabilities. For example, a small or rural health care provider must implement a solution that ensures the protection of ePHI in the manner required by the Security Rule, but the specific solution that it chooses would reflect consideration of its particular circumstances, including available resources. In some cases, a small or rural health care provider might opt to implement a cloud-based EHR or other software solution that could reduce the health care provider's need to separately invest in data storage, backup systems, and IT personnel. And in other circumstances, a small or rural health care provider might choose to contract with a third party to provide IT support, rather than hiring its own workforce members to perform such functions.

The Department also proposes to delete the maintenance provision at 45 CFR 164.306(e). Instead, as discussed in greater detail below, we propose to clearly delineate maintenance implementation specifications for specific standards, when applicable. We believe this approach would clarify how maintenance requirements relate to specific security measures and would remove any ambiguity about the need for regulated entities to regularly review, test, and modify measures as reasonable and appropriate. We further discuss maintenance provisions below for each safeguard.

4. Request for Comment

The Department requests comment on the foregoing proposals, including any benefits, drawbacks, or unintended consequences. We also request comment on the following considerations in particular:

a. Whether removing the distinction between required and addressable implementation specifications would result in unintended negative consequences for regulated entities. If so, please explain and provide a recommendation for how the Department should clarify how regulated entities are required to implement the security measures described in the proposed rule.

b. Whether the Department should include other factors in 45 CFR 164.306(b) for regulated entities to consider when selecting the security measures that they will implement to meet the requirements of the Security Rule. If so, please explain.

c. Whether the factor proposed by the Department at proposed 45 CFR 164.306(b)(2)(v) would help regulated entities identify reasonable and appropriate security measures.

d. Whether the Department's proposals sufficiently clarify that a regulated entity is expected to modify its security measures in response to changes in the environment in which health care is provided, including, but not limited to, the adoption of new technology, the evolution of existing technology, and the emergence of new threats.

e. Whether the proposals sufficiently take into account the needs and capabilities of small health care providers and rural health care providers, as required by the statute. If not, please explain and include a recommendation for ways that the Department could better account for such needs and capabilities while adequately ensuring the confidentiality, integrity, and availability of ePHI that they create, receive, maintain, or transmit. The recommendations should also take into consideration the effect of the actions taken by small and rural health care providers on the ePHI that is created, received, maintained, or transmitted by other regulated entities with whom small and rural health care providers interact.

D. Section 164.308—Administrative Safeguards

Section 164.308 of title 45 CFR contains the administrative safeguards that a regulated entity must implement, consistent with the general requirements described in 45 CFR 164.306. All of the standards and implementation specifications found in the Administrative Safeguards section refer to administrative functions, such as policies and procedures that must be in place for the management and execution of security measures.

1. Current Provisions

a. Section 164.308(a)

Section 164.308(a) contains most of the standards and associated implementation specifications that are categorized as administrative safeguards. The standards for administrative safeguards are as follows:

- Security management process.
- Assigned security responsibility.
- Workforce security.
- Information access management.
- Security awareness and training.
- Security incident procedures.
- Contingency plan.
- Evaluation.

The standard for security management process at 45 CFR 164.308(a)(1)(i) requires regulated entities to implement policies and procedures to prevent, detect, contain, and correct security violations. The Security Rule directs regulated entities as to how they are to comply with the standard for security management process through four implementation specifications. Section 164.308(a)(1)(ii)(A) requires regulated entities to conduct a risk analysis that accurately and thoroughly assesses potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI they hold. The implementation specification for risk management at 45 CFR 164.308(a)(1)(ii)(B) requires regulated entities to implement measures to reduce risks and vulnerabilities, such as those identified in the risk analysis, to a reasonable and appropriate level. Under 45 CFR 164.308(a)(1)(ii)(C), regulated entities are required to apply appropriate sanctions against workforce members who fail to comply with applicable security policies and procedures, while the implementation specification for information system activity review at 45 CFR 164.308(a)(1)(ii)(D) requires regulated entities to implement procedures to regularly review information system activity records.

The standard for assigned security responsibility at 45 CFR 164.308(a)(2) requires regulated entities to identify a security official who is responsible for the development and implementation of the policies and procedures that are required by this section. There are no implementation specifications associated with this standard.

Section 164.308(a)(3)(i) contains the standard for workforce security and requires regulated entities to implement policies and procedures to ensure that their workforce members have appropriate access to ePHI, which includes preventing workforce members who do not have authorized access from

[433] *See* 68 FR 8334, 8344 (Feb. 20, 2003).

obtaining it. The implementation specifications associated with this standard address the need to implement certain procedures regarding workforce member access to ePHI. Section 164.308(a)(3)(ii)(A) addresses the implementation of procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. The implementation specification for workforce clearance procedure at 45 CFR 164.308(a)(3)(ii)(B) addresses the implementation of procedures to determine that a workforce member's access to ePHI is appropriate, while 45 CFR 164.308(a)(3)(ii)(C) addresses the implementation of procedures for terminating a workforce member's access to ePHI when their employment or similar arrangement ends or as required by the regulated entity's workforce clearance procedures.

Under 45 CFR 164.308(a)(4)(i), the standard for information access management, a regulated entity is required to implement policies and procedures for authorizing access to ePHI in a manner that is consistent with the requirements of the Privacy Rule, that is, only when such access is appropriate based on the user or recipient's role (*i.e.,* ''role-based access''). This interpretation is consistent with the Privacy Rule's standard that limits most uses and disclosures of PHI to the ''minimum necessary'' to accomplish the purpose of the use or disclosure.[434] The standard for information access management has three implementation specifications: paragraph (a)(4)(ii)(A) requires a health care clearinghouse that is part of a larger organization to implement policies and procedures to protect ePHI from unauthorized access by that organization; paragraph (a)(4)(ii)(B) addresses implementation of policies and procedures for granting access to ePHI, for example, through a workstation, program, or other mechanism; and paragraph (a)(4)(ii)(C) addresses the implementation of policies and procedures that, based on the regulated entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, program, or other process.

Section 164.308(a)(5)(i) contains the standard for security awareness and training. This standard requires a regulated entity to implement a security awareness and training program for all workforce members, including management. There are four associated implementation specifications that address the need for regulated entities to implement the following:

- Periodic security updates.[435]
- Procedures for guarding against, detecting, and reporting malicious software.[436]
- Procedures for monitoring log-in attempts and reporting discrepancies.[437]
- Procedures for creating, changing, and safeguarding passwords.[438]

The standard for security incident procedures at 45 CFR 164.308(a)(6)(i) requires a regulated entity to implement policies and procedures to address security incidents. The one implementation specification associated with this standard, 45 CFR 164.308(a)(6)(ii), requires regulated entities to identify and respond to suspected or known security incidents; to mitigate, to the extent practicable, harmful effects of security incidents that are known to the regulated entity; and to document security incidents and their outcomes.

Under the standard for contingency planning at 45 CFR 164.308(a)(7)(i), a regulated entity is required to establish, and implement as needed, policies and procedures for responding to an emergency or other occurrence that damages systems that contain ePHI. The standard includes five implementation specifications at 45 CFR 164.308(a)(7)(ii). The first, paragraph (a)(7)(ii)(A), requires a regulated entity to establish and implement procedures to create and maintain exact copies of ePHI that are retrievable.[439] Paragraph (a)(7)(ii)(B) requires a regulated entity to establish, and implement as needed, procedures to restore any lost data.[440] Paragraph (a)(7)(ii)(C) requires a regulated entity to establish, and implement as needed, procedures to enable continuation of critical business processes for protecting the security of ePHI while the regulated entity is operating in emergency mode. Paragraph (a)(7)(ii)(D) addresses the implementation of procedures for periodic testing and revision of contingency plans, and paragraph (a)(7)(ii)(E) addresses the assessment of the relative criticality of specific applications and data in support of other contingency plan components.

The standard for evaluation at 45 CFR 164.308(a)(8) requires a regulated entity to periodically perform a technical and nontechnical evaluation that establishes the extent to which the regulated entity's security policies and procedures meet the requirements of the Security Rule. The initial evaluation is to be based upon the standards implemented under the Security Rule, while subsequent evaluations are to be conducted in response to environmental or operational changes affecting the security of ePHI.

b. Section 164.308(b)

Section 164.308(b) contains the administrative safeguards that apply to the relationships between regulated entities. Specifically, 45 CFR 164.308(b)(1) permits a covered entity to engage a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf when it obtains satisfactory assurances (consistent with the organizational requirements for business associate agreements or other arrangements in 45 CFR 164.314(a)) that the business associate will appropriately safeguard the ePHI. Similarly, under 45 CFR 164.308(b)(2), a business associate may retain a subcontractor to create, receive, maintain, or transmit ePHI on its behalf if the business associate obtains satisfactory assurances through a business associate agreement or other arrangement that the subcontractor will appropriately safeguard the information. Section 164.308(b)(3) requires that the contract or other arrangement be in writing.[441]

2. Issues To Address

The Security Rule administrative standards are comprehensive, but our experience has demonstrated that they have been misunderstood by some regulated entities, especially regarding how compliance with the standards and implementation specifications must be integrated with the general requirements in 45 CFR 164.306, including the requirement in 45 CFR 164.306(e) that a regulated entity must review and modify security measures. Section 164.306 does not explicitly reference specific security measures, and we are concerned that recent caselaw has highlighted conditions that may cause regulated entities to misinterpret regulatory text that connects the maintenance provision at 45 CFR 164.306(e) with the documentation requirements in 45 CFR 164.316 and the administrative safeguards. Through OCR's educational and enforcement efforts, we also have observed inadequacies in compliance with security management processes. For example, some regulated entities have

[434] *See* 45 CFR 164.502(b) and 164.514(d).

[435] 45 CFR 164.308(a)(5)(ii)(A).

[436] 45 CFR 164.308(a)(5)(ii)(B).

[437] 45 CFR 164.308(a)(5)(ii)(C).

[438] 45 CFR 164.308(a)(5)(ii)(D).

[439] 45 CFR 164.308(a)(7)(ii)(A).

[440] 45 CFR 164.308(a)(7)(ii)(B).

[441] 45 CFR 164.308(b)(3).

incorrectly interpreted the standards to not require implementing administrative safeguards, such as risk analyses, for all relevant electronic information systems. Some regulated entities have not documented in writing their policies, procedures, plans, and analyses.[442] As discussed above, many mistakenly treated ''addressable'' implementation standards as optional.[443] Enforcement experience has shown that regulated entities generally do not perform all elements of the risk management process that are fundamental to protecting the confidentiality, integrity, and availability of ePHI and to cybersecurity more broadly.

In addition, since the Security Rule was issued in 2003 and revised in 2013, newer, more protective security technology has become widely available to regulated entities, and best practices for securing electronic information have evolved. NIST has published numerous guides, including its recent Cybersecurity Framework 2.0, providing resources for establishing and implementing policies and practices to better manage cybersecurity risks.[444] OCR is drawing upon its enforcement experience, as well as best practices, guidelines, processes, and procedures for improving cybersecurity to propose changes to these standards to better protect ePHI that a regulated entity creates, receives, maintains, or transmits. We believe that these proposals would help ensure that regulated entities implement compliance activities that are consistent with recommendations made by NIST, the HHS 405(d) program, and standards setting bodies regarding cybersecurity.

Because business associates are directly liable for compliance with the Security Rule, in our 2013 Security Rule revisions we did not require covered entities to implement any additional safeguards to ensure that their business associate is in fact in compliance.[445] However, OCR has learned through its enforcement experience that many covered entities have entrusted ePHI to business associates that are not employing appropriate safeguards. Some business associates have such market power that covered entities may believe they have no alternative to using their services, even if they have concerns about the safeguards employed by the business associate. The Department is concerned by the breaches experienced by business associates and the effects of such breaches on the confidentiality, integrity, and availability of ePHI.[446]

3. Proposals

a. Section 164.308—Administrative Safeguards

Throughout this section, the Department proposes to add explicit maintenance requirements to certain standards to address concerns that regulated entities may be misinterpreting the regulatory text that connects the maintenance provision at 45 CFR 164.306(e) with the administrative safeguards. These proposals would clarify that a regulated entity is required to maintain certain security measures, and that where a regulated entity is required to maintain a particular security measure, it is required to review and test such measure on a specified cadence, and to modify the measure as reasonable and appropriate. Testing of particular security measures, such as technical controls or policies and procedures, would include verifying that the security measures work as designed and that workforce members know how to implement them. For example, written policies and procedures can be tested through various methods including, but not limited to: simulating security events that mimic real-world attacks to assess how effectively employees follow incident response and security procedures; conducting knowledge assessments after training on policies and procedures; and reviewing system logs and access records to evaluate whether policies and procedures governing access to ePHI are being followed. We would expect a regulated entity to take the results of the required tests into consideration when determining whether it is reasonable and appropriate to modify its security measures, as well as the actions that would be expected of a regulated entity that is similarly situated based on the results of such tests.

We also propose to modify certain administrative safeguards to clarify the obligations of a regulated entity to ensure the confidentiality, integrity, and availability of ePHI by securing its relevant electronic information systems—that is, its electronic information systems that create, receive, maintain, or transmit ePHI and those that otherwise affect its confidentiality, integrity, or availability—and the technology assets in its relevant electronic information systems.

b. Section 164.308(a)

The Department proposes to modify the general language at 45 CFR 164.308(a) to clarify the connection between the general rules for security standards at 45 CFR 164.306, the standards for policies and procedures and documentation requirements at 45 CFR 164.316, and the standards for the administrative safeguards under 45 CFR 164.308(a). We also propose to clarify that regulated entities would be required to implement all of the administrative safeguards of the Security Rule to protect the confidentiality, integrity, or availability of all ePHI that they create, receive, maintain, or transmit. Thus, when read together, proposed 45 CFR 164.308(a) and 164.316(a) would require that a regulated entity implement and document, in writing, its implementation of the administrative safeguards required by the Security Rule. These requirements set the baseline for administrative safeguards. Nothing in this NPRM would prevent a regulated entity from implementing additional administrative safeguards, provided that those additional safeguards do not conflict with any requirements in the Security Rule.

The proposed changes are discussed in greater detail below.

c. Section 164.308(a)(1)(i)—Standard: Technology Asset Inventory

We propose to modify 45 CFR 164.308(a)(1) by elevating to standard-level status the existing implementation specifications for the standard for security management process at 45 CFR 164.308(a)(1)(ii)(A) through (D), and deleting the existing standard. Doing so would highlight the importance of these elements and permit us to add implementation specifications that detail our expectations for compliance with those elements. We believe that providing more specificity in our requirements would help regulated entities better understand their compliance responsibilities for

[442] *See* proposed revisions to 45 CFR 164.316 for a more fulsome discussion of documentation requirements.

[443] *See* proposed revisions to 45 CFR 164.306(c) and (d) for a more fulsome discussion of the distinction between ''required'' and ''addressable'' implementation specifications.

[444] *See* ''The NIST Cybersecurity Framework (CSF) 2.0,'' *supra* note 15.

[445] *See* 78 FR 5566, 5572–5573 (Jan. 25, 2013) (explaining reasons for adopting proposal to apply the business associate provisions of the HIPAA Rules to subcontractors and thus, provides in the definition of ''business associate'' that a business associate includes a ''subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate'').

[446] *See, e.g.,* OCR information about the Change Healthcare cybersecurity incident. ''Change Healthcare Cybersecurity Incident Frequently Asked Questions,'' U.S. Department of Health and Human Services (July 30, 2024), *https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html.*

safeguarding ePHI. These proposals are consistent with current guidance, as described below.

In place of the existing standard for security management process, we propose a standard at 45 CFR 164.308(a)(1)(i) that would require a regulated entity to conduct and maintain an accurate and thorough written technology asset inventory and a network map of its electronic information systems and all technology assets that may affect the confidentiality, integrity, or availability of ePHI. The inventory forms the foundation for a fulsome and accurate risk analysis. A regulated entity must identify its information systems that create, receive, maintain, or transmit ePHI and all technology assets, as we propose to define them in 45 CFR 164.304, that may affect ePHI in such information systems in order to secure them. Regulated entities cannot understand the risks to the confidentiality, integrity, and availability of their ePHI without a complete understanding of these assets. We believe that this proposal would clarify compliance expectations and provide increased protections for the confidentiality, integrity, and availability of ePHI. Consistent with practices previously highlighted in guidance, regulated entities would be required by this proposal to conduct and maintain an accurate and thorough written inventory of technology assets.

The standard would also require each regulated entity to determine the movement of ePHI through, into, and out of its information systems and to describe such movement in a network map. A regulated entity's network map would reflect where its technology assets are, for example, physically located at the regulated entity's worksite, or accessed through the cloud. As another example, a covered entity might determine that ePHI is created, received, maintained, or transmitted by one or more offshore business associates (*i.e.,* persons that are located outside of the U.S.) for such services as claims processing, call center staffing, and technical support, activities that inherently involve ePHI. The technology assets used by the business associate to create, receive, maintain, or transmit ePHI are not a part of the covered entity's electronic information system, but do affect the confidentiality, integrity, or availability of ePHI and so would be required to be included in the network map of the covered entity.[447] Such assets would be considered part of the business associate's electronic information systems and therefore would need to be included in both its technology asset inventory and network map. Any technology assets used by the covered entity to create, receive, maintain, or transmit ePHI to the business associate would need to be accounted for in both its technology asset inventory and network map. Such technology assets would not be part of the business associate's technology asset inventory, but would need to be included on its network map.

This proposed standard aligns with the Department's enhanced CPG for Asset Inventory, which requires that a regulated entity identify assets to more rapidly detect and respond to potential risks and vulnerabilities,[448] and is consistent with NCVHS' recommendation to require regulated entities to identify where all PHI is stored and to collect data on applications and systems used by the organization to create a systems inventory.[449]

In 2003, the Department elected not to require regulated entities to conduct an inventory because we believed that regulated entities would understand that such an inventory is a vital component of the risk analysis, making it redundant of other requirements of the Security Rule.[450] The Department and NIST have provided extensive guidance, described below, about how to conduct such inventories as part of compliance with 45 CFR 164.308. However, nearly 20 years of enforcement experience indicates that regulated entities routinely disregard this part of the process. OCR's investigations frequently find that organizations lack sufficient understanding of where all the ePHI entrusted to their care is located.[451]

Understanding one's environment—particularly how ePHI is created and enters an organization, how ePHI flows through an organization, and how ePHI leaves an organization—is crucial to understanding the risks ePHI is exposed to throughout an organization.[452] According to the NIST Cybersecurity Framework 2.0, having a comprehensive understanding of the organization's assets (*e.g.,* data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables a regulated entity to prioritize its efforts consistent with its risk management strategy and its mission needs.[453]

The proposed standard would be accompanied by three implementation specifications. Under the proposed implementation specification for inventory at proposed 45 CFR 164.308(a)(1)(ii)(A), the regulated entity would be required to establish a written inventory that contains the regulated entity's technology assets. Technology assets are components of an electronic information system, including but not limited to hardware, software, electronic media, information, and data. The written inventory would be required to include technology assets that create, receive, maintain, or transmit ePHI and those that do not but that may affect the confidentiality, integrity, or availability of ePHI.[454] It would also be required to include the identification, version, person accountable for, and location of each of the assets or information system components.[455]

The proposed implementation specification for network map at proposed 45 CFR 164.308(a)(1)(ii)(B) would require a regulated entity to develop a network map that illustrates the movement of ePHI throughout its electronic information systems, including but not limited to how ePHI enters and exits such information systems, and is accessed from outside of such information systems.

Under the proposed implementation specification for maintenance at proposed 45 CFR 164.308(a)(1)(ii)(C), a regulated entity would be required to review and update the written inventory of technology assets and the network map in the following circumstances: (1) on an ongoing basis, but at least once every 12 months; and (2) when there is a change in the regulated entity's environment or operations that may affect ePHI. Such a change in the

[447] *See* ''Guidance on HIPAA & Cloud Computing,'' Office for Civil Rights, U.S. Department of Health and Human Services (''A covered entity (or business associate) that engages a [cloud service provider (CSP)] should understand the cloud computing environment or solution offered by a particular CSP so that the covered entity (or business associate) can appropriately conduct its own risk analysis and establish risk management policies, as well as enter into appropriate [business associate agreements.].''), *https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html.*

[448] ''Cybersecurity Performance Goals,'' *supra* note 18.

[449] *See* Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 5.

[450] *See* 68 FR 8333, 8352 (Feb. 20, 2003).

[451] *See* ''Making a List and Checking it Twice: HIPAA and IT Asset Inventories,'' Cybersecurity Newsletter, Office for Civil Rights, U.S. Department of Health and Human Services (Aug. 25, 2020), *https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-summer-2020/index.html.*

[452] *Id.*

[453] *See* ''The NIST Cybersecurity Framework (CSF) 2.0,'' *supra* note 15, p. 3.

[454] Proposed 45 CFR 164.308(a)(1)(ii)(A).

[455] *Id.*

regulated entity's environment or operations would include, but would not be limited to, the adoption of new technology assets; the upgrading, updating, or patching of technology assets; newly recognized threats to the confidentiality, integrity, or availability of ePHI; a sale, transfer, merger, or consolidation of all or part of the regulated entity with another person; a security incident that affects the confidentiality, integrity, and availability of ePHI; and relevant changes in Federal, State, Tribal, or territorial law. For example, a dissolution or bankruptcy of the regulated entity would require the regulated entity to review and update its inventory and network map. For another example, if a State implemented regulations specifying cybersecurity requirements for all hospitals, these proposed specifications would require a regulated entity in that State to review and update its inventory and network map considering implementation of the State regulations by the regulated entity or other persons whose activities may affect movement of ePHI throughout its electronic information systems.[456]

The proposed standard is consistent with the NIST Cybersecurity Framework Identify function, Asset Management (ID.AM) category, which describes inventorying hardware and software and mapping communication and data flows to create and maintain an asset inventory that can be used in a risk analysis process. For example, the Cybersecurity Framework recommends that when creating an asset inventory, organizations should include all of the following, as applicable:

- Hardware assets that comprise physical elements, including electronic devices and media, that make up an organization's networks and systems. This may include mobile devices, servers, peripherals (*e.g.,* printers, USB hubs), workstations, removable media, firewalls, and routers.
- Software assets that are programs and applications that run on an organization's electronic devices. Well-known software assets include anti-malicious software tools, operating systems, databases, email, administrative and financial records systems, electronic medical/health record systems, and clinical decision support tools, including those that rely on AI. Though lesser known, there are other programs important to IT operations and security such as backup solutions, and other administrative tools that also should be included in an organization's inventory.
- Data assets that include ePHI that an organization creates, receives, maintains, or transmits on its network, electronic devices, and media. How ePHI is used and flows through an organization is important to consider as an organization conducts its risk analysis.[457]

Where multiple persons have control over a technology asset, all persons that have control should include the asset in both their technology asset inventories and on their network maps. For example, where a covered entity contracts with a cloud-based EHR vendor, both the covered entity and the EHR vendor have control over the ePHI in the EHR. Thus, the ePHI in the EHR and the EHR should be included in the technology asset inventories and network maps of both the covered entity and the cloud-based EHR vendor. Where the technology assets are controlled entirely by another person, such as the servers controlled by a cloud-based provider of data backup services, the technology assets would not be considered part of a health care provider's electronic information systems, and therefore would not have to be included in its technology asset inventory. However, the data backup provider would have to be included in the health care provider's network map.

When creating or maintaining a technology asset inventory that can aid in identifying risks to ePHI, regulated entities should consider their technology assets that may not create, receive, maintain or transmit ePHI, but that may affect technology assets that do so.[458] Assets within an organization that do not create, receive, maintain, or transmit ePHI may still present opportunities for intruders to enter the regulated entity's electronic information systems, which could lead to risks to the confidentiality, integrity, or availability of an organization's ePHI. For example, consider a smart device that is connected to the internet (*e.g.,* connected to the Internet of Things[459] (IoT)) and provides access to facilities for maintenance personnel to control and monitor an organization's heating, ventilation, and air conditioning (HVAC). Although it may not maintain or process ePHI, such a device potentially can present serious risks to the security of ePHI in an organization's information systems. Unpatched IoT devices with known vulnerabilities, such as weak or unchanged default passwords installed on a network without firewalls, network segmentation, or other techniques that deny or impede an intruder's lateral movement, can provide an intruder with access to an organization's relevant electronic information systems. The intruder may then leverage this access to conduct reconnaissance and further penetrate an organization's network and potentially compromise ePHI.

The risks and deficiencies OCR has observed in its enforcement experience persuades us that we must consider adding an express requirement for a regulated entity to conduct an accurate and thorough written inventory of its technology assets and create a network map.

d. Section 164.308(a)(2)(i)—Standard: Risk Analysis

After a regulated entity conducts a written inventory of its technology assets and creates its network map, it is critical for it to identify the potential risks and vulnerabilities to its ePHI. Conducting a risk analysis is necessary to adequately protect the confidentiality, integrity, and availability of ePHI because it provides the basis for determining the manner in which the regulated entity will comply with and carry out the other standards and implementation specifications in the Security Rule.[460] Basic questions that a regulated entity would consider when conducting a risk analysis that is compliant with the Security Rule include:[461]

- Have you identified all the ePHI that you create, receive, maintain, or transmit?
- What are the external sources of ePHI? For example, do vendors or consultants create, receive, maintain, or transmit ePHI?
- What are the human, natural, and environmental threats to information systems that contain ePHI?

[456] *See, e.g.,* ''New York State Register,'' *supra* note 14.

[457] ''Making a List and Checking it Twice: HIPAA and IT Asset Inventories,'' *supra* note 451.

[458] *Id.*

[459] NIST defines the Internet of Things as ''[t]he network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information.'' NIST definition of ''Internet of Things,'' Glossary, Computer Security Resource Center, National Institute of Standards and Technology, U.S. Department of Commerce, *https://csrc.nist.gov/glossary/term/internet_of_things.*

[460] *See* ''Guidance on Risk Analysis,'' Office for Civil Rights, U.S. Department of Health and Human Services (July 22, 2019), *https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es.*

[461] *Id.; see also* Jeffrey A. Marron, ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' NIST Special Publication 800–66, Revision 2, National Institute of Standards and Technology, U.S. Department of Commerce, p.28–84 (Feb. 2024), *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.pdf.*

• What are the risks posed by legacy devices, including any risks that would be posed by replacing legacy devices with new ones?

There are numerous methods of performing a risk analysis, and there is no single method or ''best practice'' that guarantees compliance with the Security Rule.[462] The Department has issued multiple guidance documents and tools for regulated entities to help them implement risk analyses,[463] and several versions of its Security Risk Assessment Tool, a desktop application that walks users through the process of conducting a risk assessment.[464] NIST has published numerous guides for risk assessment over the past two decades,[465] in addition to reference materials it has developed in collaboration with the Department, including a toolkit and a crosswalk between the Security Rule to NIST Cybersecurity Framework,[466] and ''how to'' guides on risk analysis.[467] In February 2024, NIST released a new guide that provides resources for implementing a Security Rule risk analysis.[468] Consistent with previous Department guidance, the guide describes key elements in a comprehensive risk assessment process, that include the following:

• Prepare for the assessment by conducting a technology asset inventory.[469] Determine whether ePHI is transmitted to external third parties, such as cloud service providers or others. The regulated entity can also examine how access to ePHI is controlled and whether ePHI is encrypted at rest and in transit. The scope of a risk assessment should include both the physical boundaries of a regulated entity's location and a logical boundary that includes any devices or media that contain ePHI, including electronic networks through which ePHI is transmitted, regardless of its location.

• Identify reasonably anticipated threats. The list of threat events and threat sources should include reasonably anticipated and probable human and natural incidents that can negatively affect the regulated entity's ability to protect ePHI. The information gathered for the technology asset inventory should be used to identify reasonably anticipated threats to ePHI.

• Identify potential vulnerabilities and predisposing conditions. For any of the various threats identified above to result in a significant risk, each needs a vulnerability or predisposing condition that can be exploited. While it is necessary to review threats and vulnerabilities as unique elements, they are often considered at the same time. Organizations should consider a given loss scenario and evaluate both, such as what threat sources might initiate which threat events or what vulnerabilities or predisposing conditions those threat sources might exploit to cause an adverse effect. From this, the regulated entity should develop a list of vulnerabilities (*i.e.,* flaws or weaknesses) that could be exploited by potential threat sources.

• Determine the likelihood that a threat would exploit a vulnerability. For each threat event/threat source identified, a regulated entity should consider: the likelihood that the threat would occur and the likelihood that an occurred threat would exploit an identified vulnerability and result in an adverse effect. 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 an 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.

• Determine the impact of a threat exploiting a vulnerability. As with likelihood determination, a regulated entity may choose to express this effect in qualitative terms or use any other scale that the entity chooses. When selecting an impact rating, the regulated entity may consider how the threat event can affect the loss or degradation of the confidentiality, integrity, or availability of ePHI. Some tangible impacts can be measured quantitatively in terms of lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other impacts cannot be measured in specific units (*e.g.,* the loss of public confidence, the loss of credibility, or damage to an organization's interests), but they can be qualitatively described.

• Determine the level of risk to ePHI while considering the information gathered and determinations made during the previous steps. The level of risk is determined by analyzing the values assigned to the overall likelihood of threat occurrence and the resulting impact of threat occurrence.

• Document the risk assessment results. Once the risk assessment has been completed as described above, the results of the risk assessment should be documented. Principally, the regulated entity should document all threat/vulnerability pairs (*i.e.,* a scenario in which an identified threat can exploit a vulnerability) applicable to the organization, the likelihood and impact calculations, and the overall risk to ePHI for the threat/vulnerability pair. Regulated entities should consider sharing the risk assessment results with organizational leadership, whose review can be crucial to the organization's ongoing risk management.

The Department has also published guidance that explains the differences between a risk analysis and a gap analysis, and the use of both in an entity's risk management program.[470] While a risk analysis is a comprehensive identification of risks and vulnerabilities to all ePHI, a gap analysis typically provides a partial assessment of an entity's enterprise and is often used to provide a high-level overview of what safeguards are in place (or missing) and may also be used to review a regulated entity's compliance with particular standards and implementation specifications of the Security Rule.

Other NIST guidance on conducting risk assessments explains that the result of a risk analysis is a determination of risk posed to the regulated entity's ePHI and related information systems.[471]

[462] *See* ''Guidance on Risk Analysis,'' *supra* note 460.

[463] *See id.*

[464] *See* ''Security Risk Assessment Tool,'' Office for Civil Rights and Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (updated Sept. 5, 2023), *https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool.*

[465] *See* ''HIPAA Security Rule,'' National Institute of Standards and Technology, U.S. Department of Commerce (Jan. 3, 2011, updated July 21, 2022), *https://www.nist.gov/programs-projects/security-health-information-technology/hipaa-security-rule.*

[466] *See* ''HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework,'' Office for Civil Rights, U.S. Department of Health and Human Services (June 2020), *https://www.hhs.gov/guidance/sites/default/files/hhs-guidance-documents//nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf.*

[467] ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' *supra* note 461.

[468] *See id.*

[469] This component of the assessment would be accomplished under the NPRM, if adopted, through compliance with the proposed standard for technology asset inventory at proposed 45 CFR 164.308(a)(1)(i). Under the current Security Rule, we consider the technology asset inventory to be a component of the standard for risk analysis.

[470] ''Risk Analyses vs. Gap Analyses—What is the difference?'' Cybersecurity Newsletter, Office for Civil Rights, U.S. Department of Health and Human Services (Apr. 2018), *https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-april-2018.pdf.*

[471] Joint Task Force, ''Guide for Conducting Risk Assessments,'' NIST Special Publication 800–30, Revision 1, National Institute of Standards and

Continued

Consistent with the discussion above, a key step is determining the risk level posed to such ePHI by threats and vulnerabilities and how critical it is to address and mitigate the identified risk. In general, the descriptive words ''very high'' or ''critical'' are used to indicate that a threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the country.[472] A ''high'' risk would indicate that a threat event could be expected to have a severe or catastrophic adverse effect on the same, while a ''moderate'' risk could indicate that the threat event could have a serious adverse effect on the same. Risks that are ''low'' and ''very low'' could be expected to have a limited and negligible effect, respectively, on organizational operations or assets, individuals, other organizations, or the country.

The Department believes that determinations of risk level and criticality may vary based on the specific type of regulated entity and the regulated entity's specific circumstances. For example, a health care provider must consider the higher levels of risks to physical and technical security that are created by regular entry and exit of individuals seeking health care and other members of the public into its facilities, creating potentially numerous avenues for access to ePHI through technology assets; in contrast, a health plan that generally does not permit physical entry by individuals into its office building may determine that the risks to ePHI from physical entry by individuals or other members of the public is low because its workforce members do not generally physically interact with the public. As another example, a vulnerability permitting unauthenticated remote code execution on a device connected to a regulated entity's relevant electronic information systems would likely constitute either a high or critical risk. However, should such a device not have the ability to connect to the network, the risk might be low or moderate because the likelihood of triggering a network vulnerability on a non-networked device is low, even though the impact of such trigger might be high. Thus, it is essential that a regulated entity consider its specific circumstances when assessing the criticality of a risk and to address such risks in a manner that is appropriate to its specific facts and circumstances.[473] In yet another example, a regulated entity in possession of legacy devices or devices that are nearing the end of their lifespan should assess the risks associated with continued use of such devices as part of its risk analysis and ensure that replacement of such devices and/or the implementation of compensating controls are included in its risk management plan.

Despite our having made available an abundance of free and widely-publicized guidance tools, OCR unfortunately has learned through its compliance and enforcement activities that regulated entities often do not perform compliant risk analyses. As discussed above, in 2016 and 2017, the Department conducted audits of 166 covered entities and 41 business associates for their compliance with selected provisions of the HIPAA Rules.[474] These audits confirmed that only small percentages of covered entities (14 percent) and business associates (17 percent) were substantially fulfilling their regulatory responsibilities to safeguard ePHI they hold through risk analysis activities. Entities generally failed to:

- Identify and assess the risks to all of the ePHI in their possession or even develop and implement policies and procedures for conducting a risk analysis.
- Identify threats and vulnerabilities to consider their potential likelihoods and effects, and to rate the risk to ePHI.
- Review and periodically update a risk analysis in response to changes in the environment and/or operations, security incidents, or occurrence of a significant event.
- Conduct risk analyses consistent with policies and procedures.

Failing to document any efforts to develop, maintain, and update policies and procedures for conducting risk analyses was common. For example, health care providers commonly submitted documentation of some security activities performed by a third-party security vendor, without submitting documentation of any risk analysis that served as the basis of such activities.[475] Many regulated entities used and relied on outside persons to manage or perform risk analyses for their organizations; however, these outside persons frequently failed to meet the requirements of the Security Rule. Regulated entities also frequently and incorrectly assumed that a purchased security product satisfied all of the Security Rule's requirements.

The responsibility to maintain an appropriate risk analysis rests with the regulated entity. Accordingly, it is essential that regulated entities understand and comply with risk analysis requirements to appropriately safeguard PHI.

Numerous OCR investigations reflect the failure of regulated entities to develop and implement holistic risk analysis programs. For example, OCR's investigation of a health system in the aftermath of a ransomware attack found evidence of potential failures to: conduct a compliant risk analysis to determine the potential risks and vulnerabilities to ePHI in its systems; implement a contingency plan to respond to emergencies, like a ransomware attack, that damage systems that contain ePHI; and implement policies and procedures to allow only authorized users access to ePHI.[476]

In another recently concluded investigation involving a large medical center, the covered entity reported that over a seven-month period, one of its employees inappropriately accessed the ePHI of more than 12,000 patients and then sold certain patient information to an identity theft ring.[477] OCR's investigation indicated potential violations of the requirement to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all of the ePHI held by the medical center, as well as the requirement at 45 CFR 164.308(a)(1)(ii)(D) to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking.

In another case, the OCR settled a ransomware cyberattack investigation with a business associate.[478] The cyberattack affected the ePHI of over

---

Technology, U.S. Department of Commerce (Sept. 2012), *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.*

[472] *Id.* at Appendix I; *see also* ''Reducing the Significant Risk of Known Exploited Vulnerabilities,'' Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security (Nov. 3, 2021), *https://www.cisa.gov/sites/default/files/publications/Reducing_the_Significant_Risk_of_Known_Exploited_Vulnerabilities_211103.pdf.*

[473] *See* ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' *supra* note 461, p. 16–22.

[474] ''2016–2017 HIPAA Audits Industry Report,'' *supra* note 121.

[475] *Id.*

[476] Press Release, ''HHS Office for Civil Rights Settles HIPAA Security Rule Failures for $950,000,'' U.S. Department of Health and Human Services (July 1, 2024), *https://prod-wwwhhsgov.cloud.hhs.gov/about/news/2024/07/01/hhs-office-civil-rights-settles-hipaa-security-rule-failures-950000.html.*

[477] *See* ''Montefiore Medical Center,'' *supra* note 248.

[478] *See* ''Doctors' Management Services, Inc.,'' *supra* note 246.

200,000 individuals when the business associate's network server was infected with ransomware. It took the company more than 18 months to detect the intrusion, and they only did so when the ransomware was used by the intruder to encrypt the company's files. Among other factors, OCR's investigation found evidence of potential failures to conduct an accurate and thorough risk analysis and to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Given the compliance deficiencies that OCR regularly sees—those cited as examples and what OCR has observed more broadly—we believe that stronger requirements coupled with greater specificity regarding the components of a risk analysis would help and encourage regulated entities to appropriately perform such activities. Accordingly, the Department proposes to elevate the requirement to conduct a risk analysis from an implementation specification at 45 CFR 164.308(a)(1)(ii)(A) to a standard at proposed 45 CFR 164.308(a)(2)(i). Under the proposal, and consistent with NCVHS' recommendations,[479] a regulated entity would be required to conduct an accurate and comprehensive written assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI created, received, maintained, or transmitted by the regulated entity.

The Department proposes eight implementation specifications for the risk analysis standard, consistent with previously issued guidance described above. The proposed implementation specification for a written assessment at proposed paragraph (a)(2)(ii)(A) would require the regulated entity, at a minimum, to perform and document all of the following:[480]

- Review the technology asset inventory and the network map to identify where ePHI may be created, received, maintained, or transmitted within its information systems.[481]
- Identify all reasonably anticipated threats to the confidentiality, integrity, and availability of ePHI that it creates, receives, maintains, or transmits.[482]
- Identify potential vulnerabilities and predisposing conditions to the regulated entity's relevant electronic information systems—that is, its electronic information systems that create, receive, maintain, or transmit ePHI or that otherwise affect the confidentiality, integrity, or availability of ePHI.[483]
- Create an assessment and documentation of the security measures it uses to ensure that the measures protect the confidentiality, integrity, and availability of the ePHI created, received, maintained, or transmitted by the regulated entity.[484]
- Make a reasonable determination of the likelihood that each identified threat would exploit the identified vulnerabilities.[485] For example, a regulated entity located on the west coast could consult actuarial tables to reasonably determine the likelihood that an earthquake would affect access to electrical power to maintain its relevant electronic information systems.
- Make a reasonable determination of the potential impact of each identified threat should it successfully exploit the identified vulnerabilities.[486] For example, the regulated entity described above could make a reasonable determination of how and the extent to which the lack of electrical power caused by an earthquake would affect the availability and integrity of ePHI in its relevant electronic information system.
- Create an assessment of risk level for each identified threat and vulnerability.[487]
- Create an assessment of risks to ePHI posed by entering into or continuing a business associate agreement or other written arrangement with any prospective or current business associate, respectively, based on the written verification obtained from the prospective or current business associate.[488]

Under the proposed implementation specification for maintenance at proposed 45 CFR 164.308(a)(2)(ii)(B), a regulated entity additionally would be required to review, verify, and update the written assessment on an ongoing basis, but in any event no less frequently than at least once every 12 months, and in response to a change in the regulated entity's environment or operations that may affect ePHI. As discussed above, a change in the regulated entity's environment or operations that may affect ePHI would include, but would not be limited to, the adoption of new technology assets; the upgrading, updating, or patching of technology assets; newly recognized threats to the confidentiality, integrity, or availability of ePHI; a sale, transfer, merger, or consolidation of all or part of the regulated entity with another person; a security incident that affects the confidentiality, integrity, or availability of ePHI; and relevant changes in Federal, State, Tribal, or territorial law.

e. Section 164.308(a)(3)(i)—Standard: Evaluation

The Department proposes to redesignate the existing evaluation standard at 45 CFR 164.308(a)(8) as 45 CFR 164.308(a)(3)(i) and to revise the redesignated evaluation standard to require the technical and nontechnical evaluation(s) to be in writing and performed to determine whether change in the regulated entity's environment or operations may affect the confidentiality, integrity, or availability of ePHI. Evaluating the effects of a potential change on a regulated entity's environment or operations, including the effects on the confidentiality, integrity, and availability of ePHI, is a critical step in the change control process. An evaluation serves a similar purpose to a risk analysis. However, while a risk analysis looks at the entirety of a regulated entity's enterprise regularly and in response to a change in the regulated entity's environment or operations, an evaluation looks at a specific change that a regulated entity intends to make before the change is made. Thus, this proposal, if adopted, would ensure that a regulated entity proactively considers whether any risks or vulnerabilities to ePHI or its relevant electronic information systems will be introduced by changes it intends to make to its environment or operations and responds by implementing appropriate safeguards in a timely fashion.[489]

We also propose to delete the requirement that the evaluation be performed "based initially on the standards implemented under this rule" because an evaluation is performed to assess the effect(s) of a planned change on the environment, which can be observed when those effects are compared to the environment reflected in the risk analysis. Additionally, the Department proposes to add two implementation specifications at

[479] *See* Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 4–6.

[480] Proposed 45 CFR 164.308(a)(2)(ii)(A).

[481] Proposed 45 CFR 164.308(a)(2)(ii)(A)(*1*).

[482] Proposed 45 CFR 164.308(a)(2)(ii)(A)(*2*).

[483] Proposed 45 CFR 164.308(a)(2)(ii)(A)(*3*).

[484] Proposed 45 CFR 164.308(a)(2)(ii)(A)(*4*).

[485] Proposed 45 CFR 164.308(a)(2)(ii)(A)(*5*).

[486] Proposed 45 CFR 164.308(a)(2)(ii)(A)(*6*).

[487] Proposed 45 CFR 164.308(a)(2)(ii)(A)(*7*).

[488] Proposed 45 CFR 164.308(a)(2)(ii)(A)(*8*).

[489] *See* NCVHS recommendation to test at multiple points in the life cycle of a system, including "at every significant change throughout the life of the system[.]" Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 6.

proposed 45 CFR 164.308(a)(3)(ii). The proposed implementation specification for performance at proposed 45 CFR 164.308(a)(3)(ii)(A) would require that a regulated entity conduct the evaluation within a reasonable period of time before making a change to its environment or operations, while the proposed implementation specification for response at proposed 45 CFR 164.308(a)(3)(ii)(B) would require a regulated entity to respond to the evaluation in accordance with its risk management plan.

A change in the regulated entity's environment or operations would include, but would not be limited to, the adoption of new technology assets; the upgrading, updating, or patching of technology assets; newly recognized threats to the confidentiality, integrity, or availability of ePHI; a sale, transfer, merger or consolidation of all or part of the regulated entity with another person; a security incident that affects the confidentiality, integrity, or availability of ePHI; and relevant changes in Federal, State, Tribal, and territorial law.

NIST guidance provides descriptions of key activities and sample questions that would help regulated entities meet this evaluation standard.[490] They include:

- Determine whether internal or external evaluation is most appropriate. Which staff has the technical experience and expertise to evaluate the systems? If an outside vendor is used, what factors should be considered when selecting the vendor, such as credentials and experience?
- Develop standards and measurements for reviewing all standards and implementation specifications of the Security Rule. 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?
- Conduct an evaluation. 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 process?
- Document results, including: each evaluation finding and remediation options, recommendations, and decisions; known gaps between identified risks, mitigating security controls, and any acceptance of risk, including justification; developed security program priorities and established targets for continuous improvement; use of evaluation results to inform security changes to protect ePHI; communication of evaluation results, metrics, and/or measurements to relevant organizational personnel.
- Repeat evaluations periodically. Establish the frequency of evaluations, repeating evaluations when environmental and operational changes that affect the security of ePHI are made (*e.g.,* if new technology is adopted or if there are newly recognized risks to the confidentiality, integrity, or availability of ePHI).

Despite the existing standard and the availability of guidance, many regulated entities do not evaluate how changes in their environment, such as a merger or acquisition or implementation of new technology, may affect the security of ePHI. In some instances, regulated entities assert that they have done so, but have no documentation of the purported evaluation. The Department believes that this proposal, if adopted, would clarify our expectations for implementing these safeguards.

f. Section 164.308(a)(4)(i)—Standard: Patch Management

As described in Department guidance, regulated entities can defend themselves from common cyberattacks, but hackers continue to target the health care industry in search of ways to access valuable ePHI.[491] Accordingly, timely implementation of patches for known vulnerabilities is crucial to maintaining the security of ePHI. Many cyberattacks could be prevented or substantially mitigated if regulated entities implemented activities to manage the implementation of patches, updates, and upgrades to comply with the Security Rule's requirements for risk management, which can deter one of the common types of attacks: exploitation of known vulnerabilities. If an attack is successful, the intruder often will encrypt a regulated entity's ePHI to hold it for ransom, or exfiltrate the data for future purposes including identity theft or blackmail. Cyberattacks are especially concerning in the health care sector because they can disrupt the provision of health care services. Exploitable vulnerabilities can exist in many parts of a regulated entity's information systems, but often, known vulnerabilities can be mitigated by applying vendor patches, updating software or system configurations, or upgrading to a newer version of the product. If a patch, update, or upgrade is unavailable, vendors often suggest actions to take, that is, compensating controls, to mitigate a newly discovered vulnerability. Such actions could include modifications of configuration files or disabling of affected services. Regulated entities should pay careful attention to cybersecurity alerts describing newly discovered vulnerabilities. These alerts often include information on mitigation activities and patching.

Risk management processes that are compliant with the Security Rule include identifying and mitigating risks and vulnerabilities that unpatched software poses to an organization's ePHI. Mitigation activities could include installing patches if patches are available and patching is reasonable and appropriate. In situations where patches are not available (*e.g.,* obsolete or unsupported software) or testing or other concerns weigh against patching as a mitigation solution,[492] regulated entities should implement reasonable compensating controls to reduce the risk of identified vulnerabilities to a reasonable and appropriate level (*e.g.,* restricting network access or disabling network services to reduce vulnerabilities that could be exploited via network access). Security vulnerabilities may be present in many types of software, including databases, EHRs, operating systems, email, and device firmware. Each type of program would have its own unique set of vulnerabilities and challenges for applying patches, but identifying and mitigating the risks unpatched software

[490] *See* ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' *supra* note 461; ''Security Rule Guidance Material,'' Office for Civil Rights, U.S. Department of Health and Human Services (Feb. 16, 2024), *https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html?language=es.*

[491] *See* ''Defending Against Common Cyber-Attacks,'' *supra* note 396.

[492] It may not be reasonable and appropriate for a regulated entity to patch software or update a system configuration where the risk of introducing a change is greater than the status quo risk or where the regulated entity does not own or manage a networked device. For example, instances where it might not be reasonable and appropriate to patch or update an information system include: (1) where a system needs to run continuously for mission critical support and is not patched or updated during its lifetime; and (2) where the regulated entity's testing of such patch or update indicates potential adverse impacts or where industry is reporting adverse impacts of such patch or update. This does not negate the regulated entity's need to address the vulnerability with a compensating control. For example, where a hospital discovers a vulnerability on a device that is connected to its network but owned and managed by a business associate, the hospital may not have access to install a patch, but it should employ a compensating control, such as disabling or limiting that device's access to the hospital's network.

poses to ePHI is important to ensuring that ePHI is protected.[493]

Although older applications or devices may no longer be supported with patches for new vulnerabilities, regulated entities must still take appropriate action if a newly discovered vulnerability affects an older application or device. If an obsolete, unsupported system cannot be upgraded or replaced, additional safeguards should be implemented or existing safeguards enhanced to mitigate known vulnerabilities until upgrade or replacement can occur (*e.g.,* increase access restrictions, remove or restrict network access, disable unnecessary features or services).[494]

Patches can be applied to software and firmware on all types of devices—telephones, computers, servers, routers, and more. Installation of vendor-recommended patches is typically a routine process. However, regulated entities should be prepared if issues arise as a result of applying patches. Software and hardware are often interconnected and dependent on the functionality and output of other information systems or components of other information systems. When certain changes are made, including the installation of a patch, software dependent on the changed application may not perform as expected because settings or data may be affected. Thus, in complex environments, patch management plays a crucial role in the safe and correct implementation of these changes.[495] Enterprise patch management is the process of identifying, prioritizing, acquiring, installing, and verifying the installation of patches, updates, and upgrades throughout an organization.[496] NIST has issued a series of guidance documents that regulated entities can use to design their own patch management processes as part of their risk management plans.

Consistent with previously issued guidance, the discussion above, and recommendations from NCVHS,[497] the Department proposes a new standard for patch management at proposed 45 CFR 164.308(a)(4)(i) that would require a regulated entity to implement written policies and procedures for applying patches and updating the configurations of its relevant electronic information systems. This proposed standard would ensure that a regulated entity is aware of its liability for appropriately safeguarding ePHI by installing patches, updates, and upgrades throughout its relevant electronic information systems.

The Department proposes six implementation specifications at proposed 45 CFR 164.308(a)(4)(ii) that would be associated with the proposed standard for patch management. The proposed implementation specification for policies and procedures at proposed paragraph (a)(4)(ii)(A) would require a regulated entity to establish written policies and procedures for identifying, prioritizing, acquiring, installing, evaluating, and verifying the timely installation of patches, updates, and upgrades throughout its electronic information systems that create, receive, maintain, or transmit ePHI or that otherwise affect the confidentiality, integrity, or availability of ePHI. Under the proposed implementation specification for maintenance at proposed paragraph (a)(4)(ii)(B), a regulated entity would be required to review its patch management written policies and procedures at least once every 12 months and modify them as reasonable and appropriate based on that review. The proposed implementation specification for application at proposed paragraph (a)(4)(ii)(C) would require a regulated entity to patch, update, and upgrade the configurations of its relevant electronic information systems in accordance with its written policies and procedures and based on the results of: the regulated entity's risk analysis that would be required by proposed 45 CFR 164.308(a)(2), the vulnerability scans that would be required under proposed 45 CFR 164.312(h)(2)(i), the monitoring of authoritative sources that would be required under proposed 45 CFR 164.312(h)(2)(ii), and penetration tests proposed at 45 CFR 164.312(h)(2)(iii). The proposal would require that such actions be taken within a reasonable and appropriate period of time, except to the extent that an exception in proposed paragraph (h)(2)(ii)(D) applies. Specifically, a reasonable and appropriate period of time to patch, update, or upgrade the configuration of a relevant electronic information system would be within 15 calendar days of identifying the need to address a critical risk where a patch, update, or upgrade is available; or, where a patch, update, or upgrade is not available, within 15 calendar days of a patch, update, or upgrade becoming available. The proposal would require that, within 30 calendar days of identifying the need to address a high risk,[498] a regulated entity patch, update, or upgrade the configuration of a relevant electronic information system where a patch, update, or upgrade is available; or, where a patch, update, or upgrade is not available, within 30 calendar days of a patch, update, or upgrade becoming available. For all other patches, updates, or upgrades to the configurations of relevant electronic information systems, a reasonable and appropriate period of time would be determined by the regulated entity's written policies and procedures for identifying, prioritizing, acquiring, installing, evaluating, and verifying the timely installation of patches, updates, and upgrades.

For the proposed exceptions to apply, we propose in proposed paragraph (a)(4)(ii)(D) that a regulated entity would be required to document that an exception applies and that all other applicable conditions are met. The first proposed exception in proposed 45 CFR 164.308(a)(4)(ii)(D)(*1*) would be for when a patch, update, or upgrade to the configuration of a relevant electronic information system is not available to address a risk identified in the regulated entity's risk analysis. The second proposed exception would be in proposed 45 CFR 164.308(a)(4)(ii)(D)(*2*) for when the only available patch, update, or upgrade would adversely affect the confidentiality, integrity, or availability of ePHI. The Department anticipates that this proposed exception would apply when a regulated entity tests a patch, update, or upgrade and determines that it would adversely affect the confidentiality, integrity, or availability of ePHI or where there are reports from government sources or persons with appropriate knowledge of an experience with generally accepted cybersecurity principles and methods for ensuring the confidentiality, integrity, and availability of ePHI indicating that the patch, update, or

[493] *See* ''Guidance on Software Vulnerabilities and Patching,'' Cybersecurity Newsletter, Office for Civil Rights, U.S. Department of Health and Human Services (June 2018), *https://www.hhs.gov/sites/default/files/june-2018-newsletter-software-patches.pdf.*

[494] *See* ''Securing Your Legacy [System Security],'' Cybersecurity Newsletter, Office for Civil Rights, U.S. Department of Health and Human Services (Oct. 2021), *https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-fall-2021/index.html.*

[495] *See* ''Guidance on Software Vulnerabilities and Patching,'' *supra* note 493.

[496] *See* Murugiah Souppaya, et al., ''Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology,'' NIST Special Publication 800–40, Revision 4, National Institute of Standards and Technology, U.S. Department of Commerce (Apr. 2022), *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf.*

[497] Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 1; Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123, p. 8–9.

[498] An explanation of risk rating is provided above in the discussion of the proposed standard for risk analysis and associated implementation specifications.

upgrade is likely to adversely affect the confidentiality, integrity, or availability of ePHI.

In proposed paragraph (a)(4)(ii)(E), the Department proposes to require a regulated entity document in real-time the existence of the applicable exception and to implement reasonable and appropriate compensating controls. Similarly, in proposed paragraph (a)(4)(ii)(F), we propose that, where an exception applies, a regulated entity would be required to implement reasonable and appropriate security measures as compensating controls to address the identified risk according to the timeliness requirements in proposed 45 CFR 164.308(a)(5)(ii)(D) until such time as a patch, update, or upgrade that does not adversely affect the confidentiality, integrity, or availability of ePHI becomes available.

This proposed standard aligns with the Department's enhanced CPG for Cybersecurity Mitigation by quickly requiring a regulated entity to prioritize and mitigate vulnerabilities discovered by vulnerability scanning and penetration testing.[499]

g. Section 164.308(a)(5)(i)—Standard: Risk Management

The Department proposes to elevate the implementation specification for risk management to a standard at proposed 45 CFR 164.308(a)(5)(i). This proposed standard would require a regulated entity to establish and implement a plan for reducing the risks identified through its risk analysis activities. Specifically, it would require a regulated entity to implement security measures sufficient to reduce risks and vulnerabilities to all ePHI to a reasonable and appropriate level. What would constitute a reasonable and appropriate level depends on the regulated entity's specific circumstances, including but not limited to its size, needs and capabilities, risk profile, the ability of security measures to reduce or eliminate a particular identified risk or vulnerability, and the ubiquity of such security measures. We also propose four implementation specifications that would require regulated entities to engage in activities that are consistent with previously issued guidance described below.

Under the proposed implementation specification for planning at proposed paragraph (a)(5)(ii)(A), a regulated entity would be required to establish and implement a written risk management plan for reducing risks to all ePHI, including, but not limited to, those risks identified by the regulated entity's risk analysis,[500] to a reasonable and appropriate level. Proposed paragraph (a)(5)(i)(B) contains the proposed implementation specification for maintenance and would require the regulated entity to review the written risk management plan at least once every 12 months, and as reasonable and appropriate in response to changes in its risk analysis. The Department would interpret ''reasonable and appropriate'' in both paragraphs as requiring the regulated entity to take into account not only its specific circumstances, but also the criticality of the risks identified. We propose an implementation specification for priorities at proposed 45 CFR 164.308(a)(5)(ii)(C) that would require a regulated entity's written risk management plan to prioritize the risks identified in the regulated entity's risk analysis based on the risk levels determined by that analysis. Finally, in the proposed implementation specification for implementation at proposed 45 CFR 164.308(a)(5)(ii)(D), we propose to require that a regulated entity implement security measures in a timely manner to address the risks identified in the regulated entity's risk analysis in accordance with the priorities established under paragraph (a)(5)(ii)(C). The proposed risk management standard aligns with the Department's essential CPG to Mitigate Known Vulnerabilities.[501]

The Department previously issued guidance on risk management, including links to NIST resources, that is consistent with what we propose in this NPRM.[502] We encourage regulated entities to refer to similar NIST guidance for descriptions of risk management activities.[503] The results of a risk analysis, performed in accordance with the proposed standard for risk analysis, generally provide the regulated entity with a list of applicable ''threat/vulnerability pairs'' as well as the overall ''risk rating'' of each pair to the confidentiality, integrity, and availability of ePHI.[504] For example, some threat/vulnerability pairs may result in a risk rating of moderate or high level of risk to ePHI, while other pairs may result in a risk rating of low level of risk. The regulated entity would need to determine what risk rating poses an unacceptable level of risk to ePHI and address any threat/vulnerability pairs that indicate a risk rating above the organization's risk tolerance.[505]

Under this proposed standard, the regulated entity would be required to reduce the risks to its ePHI to a level that is reasonable and appropriate for its specific circumstances. Ultimately, the regulated entity's risk assessment processes should inform its decisions about the manner in which it will implement security measures to comply with the Security Rule's standards and implementation specifications.[506] Additionally, each regulated entity would be required to document the security controls it has implemented because it has determined them to be reasonable and appropriate, including analyses, decisions, and the rationale for decisions made to refine or adjust the security controls.[507]

As stated by NIST, ''the documentation and retention of risk assessment and risk management activities'' is ''important for future risk management efforts.'' [508] In general, risk management activities ''should be performed with regular frequency to examine past decisions, reevaluate risk likelihood and impact levels, and assess the effectiveness of past remediation efforts.'' [509] Risk management plans should address risk appetite, risk tolerance, workforce duties, responsible parties, the frequency of risk management, and required documentation.[510]

h. Section 164.308(a)(6)(i)—Standard: Sanction Policy

Consistent with other proposals to elevate certain critical implementation specifications to standards, we propose to elevate the implementation specification for sanction policy at 45 CFR 164.308(a)(ii)(C) to a standard for sanction policy at proposed 45 CFR 164.308(a)(6)(i). We propose this standard because applying appropriate sanctions against workforce members who fail to comply with security requirements, and thus imperil the

[499] ''Cybersecurity Performance Goals,'' *supra* note 18.

[500] *See* proposed 45 CFR 164.308(a)(2).

[501] ''Cybersecurity Performance Goals,'' *supra* note 18.

[502] *See* ''6 Basics of Risk Analysis and Risk Management,'' HIPAA Security Series, Volume 2, Paper 6, Centers for Medicare & Medicaid Services (June 2005, revised Mar. 2007), *https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf?language=es.*

[503] *See* ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' *supra* note 461.

[504] *See id.* at 18.

[505] *See id.* at 25.

[506] *Id.*

[507] *See* proposed 45 CFR 164.306(d) and 164.316(b)(1).

[508] *See* ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' *supra* note 461, p. 27.

[509] *See id.* at 31.

[510] *See id.*

security of ePHI, serves as an important tool for improving compliance by other workforce members with the regulated entity's safeguards for ePHI. While the Department does not propose to modify the language of the standard, we are proposing three implementation specifications that are consistent with guidance that was previously issued by the Department.

Specifically, under the proposed implementation specification for policies and procedures at proposed 45 CFR 164.308(a)(6)(ii)(A), a regulated entity would be required to establish written policies and procedures for sanctioning workforce members who fail to comply with the regulated entity's security policies and procedures. The proposed implementation specification for modifications at paragraph (a)(6)(ii)(B) would require a regulated entity to review its written sanctions policies and procedures at least once every 12 months, and, based on that review, modify such policies and procedures as reasonable and appropriate. The proposed implementation specification for application at proposed paragraph (a)(6)(ii)(C) would direct a regulated entity to apply appropriate sanctions against workforce members who fail to comply with such security policies and procedures and to document when it sanctions a workforce member and the circumstances in which it applies such sanctions.

The policy choices represented in this NPRM are informed by the compliance challenges OCR has observed through its enforcement activities. These challenges demonstrate that regulated entities would benefit from greater precision and clarity about their legal obligations in the proposed standard. Additionally, according to a recent survey of IT and IT security practitioners in healthcare, careless users were the top cause of data loss and exfiltration, while accidental loss was the second highest cause. Thirty-one percent of respondents indicated that the data loss or exfiltration was caused by a failure of workforce members to follow organizational policies.[511] As described in existing Department guidance, an organization's sanction policies can be an important tool for supporting accountability and improving cybersecurity and data protection.[512] Sanction policies can be used to address the intentional actions of malicious insiders, such as a workforce member that accesses the ePHI of a public figure or steals ePHI to sell as part of an identity-theft ring, as well as the failure of workforce members to comply with policies and procedures, such as failing to secure data on a network server or investigate a potential security incident.

Sanction policies that are appropriately applied can improve a regulated entity's general compliance with the HIPAA Rules. Imposing consequences on workforce members who violate a regulated entity's policies and procedures implemented as required by the Security Rule or the HIPAA Rules generally can be effective in creating a culture of HIPAA compliance and improved cybersecurity. Knowledge that there is a negative consequence to noncompliance enhances the likelihood of compliance.[513] Training workforce members on a regulated entity's sanction policy can also promote compliance and greater cybersecurity vigilance by informing workforce members in advance which actions are prohibited and punishable.[514] A sanction policy that clearly communicates a regulated entity's expectations should ensure that workforce members understand their individual compliance obligations and consequences of noncompliance.

Regulated entities have the flexibility to implement the standard in a manner consistent with numerous factors, including but not limited to their size, degree of risk, and environment. The HIPAA Rules do not require regulated entities to impose any specific penalty for any particular violation, nor do they require regulated entities to implement any particular methodology for sanctioning workforce members. Rather, in any particular case, each regulated entity must determine the type, cause, and severity of sanctions imposed based upon its policies and the relative severity of the violation.[515] A regulated entity may structure its sanction policies in the manner most suitable to its organization. As described in previously issued guidance materials from the Department and NIST, regulated entities should consider the following when drafting or revising their sanction policies:

- Documenting or implementing sanction policies pursuant to a formal process.[516]
- Requiring workforce members to affirmatively acknowledge that a violation of the organization's HIPAA policies or procedures may result in sanctions.[517]
- Documenting the sanction process, including the personnel involved, the procedural steps, the time-period, the reason for the sanction(s), and the final outcome of an investigation.[518]
- Creating sanctions that are ''appropriate to the nature of the violation.'' [519]
- Creating sanctions that ''vary depending on factors such as the severity of the violation, whether the violation was intentional or unintentional, and whether the violation indicated a pattern or practice of improper use or disclosure of [PHI].'' [520]
- Creating sanctions that ''range from a warning to termination.'' [521]
- Providing examples ''of potential violations of policy and procedures.'' [522]

Generally, it is important for a regulated entity to consider whether its sanction policies align with its general disciplinary policies, and how the individuals or departments involved in the sanction processes can work in concert, when appropriate. Regulated entities may also want to consider how sanction policies can be fairly and consistently applied throughout the organization, to all workforce members, including management.[523] The deterrent effect of penalizing noncompliance and misconduct paired with clear communications about the consequences of noncompliance can promote greater compliance with the HIPAA Rules through accountability, understanding, and transparency.

[511] ''The 2024 Study on Cyber Insecurity in Health Care: The Cost and Impact on Patient Safety and Care,'' *supra* note 143, p. 7.

[512] *See* ''How Sanction Policies Can Support HIPAA Compliance,'' Cybersecurity Newsletter, Office for Civil Rights, U.S. Department of Health and Human Services (Oct. 2023), *https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-october-2023/index.html#ftn10.*

[513] 68 FR 8334, 8347 (Feb. 20, 2003).

[514] 65 FR 82462, 82747 (Dec. 28, 2000).

[515] 68 FR 8334, 8347 (Feb. 20, 2003).

[516] 65 FR 82462, 82562 (Dec. 28, 2000).

[517] *See* ''Security Standards: Administrative Safeguards,'' HIPAA Security Series, Volume 2, Paper 2, Centers for Medicare & Medicaid Services (May 2005, revised Mar. 2007), *https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf; see also* ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' *supra* note 461, p. 33.

[518] Records of sanction activity should be retained for at least six years. *See* 45 CFR 164.316 and 164.530(e)(2).

[519] *See* 65 FR 82462, 82562 (Dec. 28, 2000).

[520] *Id.*

[521] *Id.*

[522] *See* ''Security Standards: Administrative Safeguards,'' *supra* note 517.

[523] *See* 45 CFR 164.308(a)(1)(ii)(C), 164.530(e)(1); *see also* 65 FR 82462, 82747 (Dec. 28, 2000) (''All members of a covered entity's workforce are subject to sanctions for violations.'').

i. Section 164.308(a)(7)(i)—Standard: Information System Activity Review

As described in previously issued HHS guidance, review of activity in its relevant electronic information systems and their components, including workstations,[524] enables a regulated entity to determine if any ePHI has been used or disclosed in an inappropriate manner.[525] The procedures should be customized to meet the regulated entity's risk management strategy and consider the capabilities of all information systems with ePHI.[526] These activities should also promote continual awareness of any information system activity that could suggest a security incident.[527]

Detecting and preventing data leakage initiated by malicious authorized users is a significant challenge.[528] Identifying potential malicious activity in relevant electronic information systems, including in workstations and other components, as soon as possible is key to preventing or mitigating the impact of such activity.[529] To identify potential suspicious activity, organizations should consider an insider's interactions with information systems and their components. A regulated entity can detect anomalous user behavior or indicators of misuse by either a trusted employee or third-party vendor who has access to critical systems, workstations and other system components, and data.[530] To minimize this risk, an organization may employ safeguards that detect suspicious user activities, such as traffic to an unauthorized website, downloading data to an external device (*e.g.,* thumb drive), or access to a network server by an unauthorized mobile device. Maintaining audit controls (*e.g.,* system event logs, application audit logs) and regularly reviewing audit logs, access reports, and security incident tracking reports are important security measures that can assist in detecting and identifying suspicious activity or unusual patterns of data access.[531]

Regulated entities should regularly review activity in their relevant electronic information systems (including the components of such systems) for potential concerns and consider ways to automate such reviews.[532] Additionally, regulated entities are responsible for establishing and implementing appropriate standard operating procedures, including determining the types of audit trail data and monitoring procedures that would be needed to derive exception reports.[533] They also must activate the necessary review processes and maintain auditing and logging activity.[534]

Department and NIST guidance advise regulated entities to consider many questions when establishing their policies and procedures for reviewing activity in their relevant electronic information systems review.[535] These include:

- What logs or reports are generated by the information systems?
- 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?
- How often will review results be analyzed?
- Where will audit information reside (*e.g.,* separate server)? Will it be stored external to the organization (*e.g.,* cloud service provider)?

Compliance challenges observed through OCR's enforcement activities suggest that regulated entities would benefit from an expanded standard to provide more details on compliance expectations. Investigations of reported breaches of unsecured PHI discussed above as examples of risk analysis failures also identified a potential failure by the regulated entities to conduct appropriate information system activity review.[536] In an investigation involving a large health care provider, the ePHI of more than 12,000 patients was sold to an identity theft ring by employees who, for six months, inappropriately accessed patient account information.[537] Compliance with the requirement to implement procedures to regularly review records of activity in relevant electronic information systems, such as audit logs, access reports, and security incident tracking, could have identified and mitigated these disclosures.[538]

Similarly, a business associate experienced an intrusion into its systems that it failed to notice for over 20 months. Eventually, the ePHI of more than 200,000 individuals associated with several covered entities was encrypted in a ransomware cyberattack.[539] Among other factors, OCR's investigation indicated that the business associate potentially failed to implement procedures for regularly reviewing records of activity in its relevant electronic information system, such as audit logs, access reports, and security incident tracking reports.[540]

Consistent with previously issued guidance and based on OCR's enforcement experience, the Department proposes to elevate the existing implementation specification for information system activity review to a standard and to redesignate it as proposed 45 CFR 164.308(a)(7)(i). The purpose of the proposal is to impose specific requirements on a regulated entity to review the activity occurring in its relevant electronic information systems, including the activity occurring in the components of such systems. By virtue of these proposed requirements, we would specify actions that a regulated entity is required to take to ensure that only appropriate users access ePHI and that it responds quickly to any suspicious activity in its relevant electronic information systems, including in components thereof, such as workstations that connect to or otherwise access its relevant electronic information systems. We also propose to revise the language to provide regulated entities with additional direction regarding their review of suspicious activities. The proposed standard, if adopted, would require a regulated entity to implement written policies and procedures for regularly reviewing

[524] Workstations may also be referred to as ''endpoints.'' *See* ''Memorandum on Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response,'' Office of Management and Budget, Executive Office of the President, p. 1 (Oct. 8, 2021) *https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf.*

[525] *See* ''Security Standards: Administrative Safeguards,'' *supra* note 517, p. 5–6.

[526] *See id.* at 6.

[527] *Id.*

[528] *See* ''Managing Malicious Insider Threats,'' Cybersecurity Newsletter, Office for Civil Rights, U.S. Department of Health and Human Services (Aug. 2019), *https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-summer-2019/index.html.*

[529] *Id.*

[530] *Id.*

[531] *Id.*

[532] *See* ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' *supra* note 461, p. 33.

[533] *See id.* at 34.

[534] *See id.*

[535] *See* ''Security Standards: Administrative Safeguards,'' *supra* note 517, p. 7; *see also* ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' *supra* note 461, p. 30–34.

[536] *See* Press Release, ''HHS Office for Civil Rights Settles HIPAA Security Rule Failures for $950,000,'' U.S. Department of Health and Human Services (July 1, 2024), *https://prod-wwwhhsgov.cloud.hhs.gov/about/news/2024/07/01/hhs-office-civil-rights-settles-hipaa-security-rule-failures-950000.html.*

[537] *See* ''Montefiore Medical Center,'' *supra* note 248.

[538] *See* 45 CFR 164.308(a)(1)(ii)(D).

[539] *See* ''Doctors' Management Services, Inc.,'' *supra* note 246.

[540] *Id.*

records of activity in its relevant electronic information systems.

The Department proposes five implementation specifications for the proposed standard for information system activity review. The proposed implementation specification for policies and procedures at proposed 45 CFR 164.308(a)(7)(ii)(A) would require a regulated entity to establish written policies and procedures for retaining and reviewing records of activity in the regulated entity's relevant electronic information systems by persons and technology assets. Such written policies and procedures should require review of activity in the regulated entity's relevant electronic information systems as a whole, as well as the system's components, including but not limited to any workstations. They should also include information on the frequency for reviewing such records. The frequency of review may vary based on the specific type of record being reviewed and the information it contains. According to the proposed implementation specification for scope at proposed 45 CFR 164.308(a)(7)(ii)(B), records of activity in the regulated entity's relevant electronic information systems by persons and technology assets would include, but would not be limited to, audit trails, event logs, firewall logs, system logs, data backup logs, access reports, anti-malware logs, and security incident tracking reports. The proposed implementation specification for records review at proposed 45 CFR 164.308(a)(7)(ii)(C) would require a regulated entity to review records of activity in its relevant electronic information systems by persons and technology assets as often as reasonable and appropriate for the type of report or log. They would also be required to document such review. A proposed implementation specification for record retention at proposed 45 CFR 164.308(a)(7)(ii)(D) would require a regulated entity to retain records of activity in its relevant electronic information systems by persons and technology assets. Under the proposal, the regulated entity would be required to retain such records for an amount of time that is reasonable and appropriate for the specific type of report or log. For example, it may be reasonable and appropriate to retain audit trails for a different amount of time than security incident tracking reports because of the type of information they contain and their purpose. The proposed implementation specification for response at proposed 45 CFR 164.308(a)(7)(ii)(E) would require a regulated entity to respond to a suspected or known security incident identified during the review of activity in its relevant electronic information systems, including any components thereof, such as workstations, in accordance with the regulated entity's security incident plan.[541] Finally, the proposed implementation specification for maintenance at proposed 45 CFR 164.308(a)(7)(ii)(F) would require a regulated entity to review and test its written policies and procedures for reviewing activity in its relevant electronic information systems at least once every 12 months. The regulated entity would be expected to modify such policies and procedures as reasonable and appropriate, based on the results of that review.

Consider a large regulated entity that may have thousands of workforce members accessing various networks and relevant electronic information systems, generating large amounts of log and audit data. Given the size, complexity, and capabilities of entities of such size, a reasonable and appropriate process for reviewing activity may include the adoption of an automated solution that performs rules-based enterprise log aggregation and analysis to identify anomalous or suspicious patterns of behavior in the regulated entity's relevant electronic information systems and the components thereof, including but not limited to workstations, in real-time and sends alerts of potential security incidents to a workforce member or team for further review and action. By contrast, for a small regulated entity, it might be reasonable and appropriate to have designated staff that manually review log files and audit trails multiple times per week.

j. Section 164.308(a)(8)—Standard: Assigned Security Responsibility

The Department proposes to redesignate the standard for assigned security responsibility at 45 CFR 164.308(a)(2) as proposed 45 CFR 164.308(a)(8). OCR's enforcement experience demonstrates that, in practice, many regulated entities follow informal policies and procedures that are not documented, and have not documented the identification of the Security Official in writing.

Based on OCR's enforcement experience, and consistent with existing guidance, we propose to modify the standard to specify that a regulated entity must identify in writing the Security Official who is responsible for the establishment and implementation of the policies and procedures, whether written or otherwise, and deployment of technical controls. These proposals are consistent with our general intention in this NPRM to propose to clarify that policies and procedures required by the Security Rule should be reduced to writing and to distinguish between the implementation of written policies and procedures and the deployment of technical controls.

As we previously explained in guidance,[542] the purpose of this standard is to identify who would be operationally responsible for assuring that the regulated entity complies with the Security Rule. It is comparable to the Privacy Rule standard for personnel designations at 45 CFR 164.530(a)(1), which requires all covered entities to designate a Privacy Official. The Security Official and Privacy Official can, but need not be, the same person. While one workforce member must be designated as having overall responsibility, other workforce members may be assigned specific security responsibilities (*e.g.,* facility security, network security). When making this decision, regulated entities should consider basic questions, such as: Has the organization agreed upon, and clearly identified and documented, the responsibilities of the Security Official? How are the roles and responsibilities of the Security Official crafted to reflect the size, complexity, and technical capabilities of the organization?

NIST guidance urges the regulated entity to select a workforce member who is able to assess the effectiveness of security to serve as the point of contact for security policy, implementation, and monitoring.[543] It further recommends that a regulated entity should document the responsibilities in a job description and communicate this assigned role to the entire organization. NIST provides additional sample items for consideration by a regulated entity organizing its security practices, including identifying the workforce members in the organization who oversee the development and communication of security policies and procedures, direct IT security purchasing and investment, and ensure that security concerns have been addressed in system implementation. NIST also offers that a regulated entity should ask whether the security official has adequate access and communications with senior officials in the organization and whether there is a

[541] *See* proposed 45 CFR 164.308(a)(12)(ii)(B).

[542] *See* ''Security Standards: Administrative Safeguards,'' *supra* note 517, p. 7.

[543] *See* ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' *supra* note 461.

complete job description that accurately reflects assigned security duties and responsibilities.

k. Section 164.308(a)(9)(i)—Standard: Workforce Security

The purpose of the workforce security standard is to ensure that workforce members only have access to ePHI that they need to perform their assigned functions and are prevented from accessing ePHI that they are not authorized to access to perform such functions. The proposed changes to the standard and implementation specifications would clarify the actions required of a regulated entity to assure such limits.

Individuals have been harmed in the past by the failure of regulated entities to comply with the Security Rule requirements for workforce security. For example, a former employee of a large covered entity was able to access their former worksite and workstation using still-active credentials for more than a week after their employment was terminated.[544] OCR's investigation found evidence of a potential failure to terminate the former employee's access to PHI, which enabled the former employee to download the ePHI of nearly 500 individuals, including their names, addresses, dates of birth, race/ethnicity, gender, and sexually transmitted infection test results onto a USB drive. This type of real-world experience and OCR's observations more broadly inform the changes proposed in this NPRM.

Moreover, this proposal is consistent with guidance issued by HHS and NIST for implementing this standard and associated implementation specifications. For example, in guidance issued in 2005, we explained that regulated entities must identify workforce members who need access to ePHI to carry out their duties.[545] For each workforce member or job function, the regulated entity must identify the ePHI that is needed, when it is needed, and make reasonable efforts to control access to the ePHI, a concept generally referred to as role-based access (*i.e.,* authorizing access to ePHI only when such access is appropriate based on the workforce member's role).[546] This also includes identification of the computer systems and applications that provide access to the ePHI. A regulated entity must provide only the minimum necessary access to ePHI that is required for a workforce member to do their job.[547] As described in HHS guidance, access authorization is the process of determining whether a particular user (or a computer system) has the right, consistent with their function, to carry out a certain activity, such as reading a file or running a program.[548] Implementation may vary among regulated entities, depending on the size and complexity of their workforce, and their electronic information systems that contain ePHI. For example, in a small medical practice, all staff members may need to access all ePHI in their information systems because each staff member may perform multiple functions. In this case, the regulated entity would document the reasons for implementing policies and procedures that permit this type of global access. If the documented rationale is reasonable and appropriate, this may be an acceptable approach. The implementation specification provision for authorization and/or supervision provides the necessary checks and balances to ensure that all members of the workforce have appropriate access (or, in some cases, no access) to ePHI.

NIST guidance provides descriptions of key activities and sample questions for regulated entities implementing this implementation specification.[549] To implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed, the guidance advises regulated entities to consider whether chains of command and lines of authority have been established, as well as the identity and roles of supervisors. A regulated entity also should establish clear job descriptions and responsibilities, which includes defining roles and responsibilities for all job functions; assigning appropriate levels of security oversight, training, and access; and identifying 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.[550] To determine the most reasonable and appropriate authorization and/or supervision procedures, a regulated entity must be able to answer some basic questions about existing policies and procedures. For example, are detailed job descriptions used to determine what level of access the person holding the position should have to ePHI? Who has or should have the authority to determine who can access ePHI, *e.g.,* supervisors or managers? Are there written job descriptions that are correlated with appropriate levels of access to ePHI? Are these job descriptions reviewed and updated on a regular basis? Have workforce members been provided copies of their job descriptions and informed of the access granted to them, as well as the conditions by which this access can be used? As noted above, a smaller regulated entity may address compliance by implementing a simpler approach, but it is still liable for ensuring that workforce members only have access to ePHI that they need to perform their assigned functions.[551]

NIST also recommends establishing criteria and procedures for hiring and assigning tasks and ensuring that these requirements are included as part of the personnel hiring process.[552] In its guidance, NIST provides questions and suggestions for regulated entities to consider with respect to these criteria, procedures, and requirements. NIST guidance also describes this implementation specification as calling for regulated entities to implement appropriate screening of persons who would have access to ePHI, and a procedure for obtaining clearance from appropriate offices or workforce members where access is provided or terminated.[553] Similarly, the Department's guidance on workforce clearance procedures states that the clearance process must establish the procedures to verify that a workforce member would in fact have the appropriate access for their job function.[554] A regulated entity may choose to perform this type of screening procedure separate from, or as a part of, the authorization and/or supervision procedure. Sample questions for

[544] *See* Press Release, ''City Health Department failed to terminate former employee's access to protected health information,'' U.S. Department of Health and Human Services (Oct. 30, 2020), *https://public3.pagefreezer.com/content/HHS.gov/31-12-2020T08:51/https://www.hhs.gov/about/news/2020/10/30/city-health-department-failed-terminate-former-employees-access-protected-health-information.html.*

[545] *See* ''Security Standards: Administrative Safeguards,'' *supra* note 517, p. 8–11.

[546] *See* ''Summary of the HIPAA Security Rule,'' U.S. Department of Health and Human Services (Oct. 19, 2022), *https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.*

[547] *See* 45 CFR 164.502(b) and 164.514(d).

[548] *See* ''Security Standards: Administrative Safeguards,'' *supra* note 517, p. 9.

[549] *See* ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' *supra* note 461.

[550] *See id.* at 36.

[551] *See* proposed 45 CFR 164.308(a)(9)(i).

[552] *See* ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' *supra* note 461, p. 36.

[553] *See id.*

[554] *See* ''Security Standards: Administrative Safeguards,'' *supra* note 517, p. 10.

regulated entities to consider include the following: Are there existing procedures for determining that the appropriate workforce members have access to the necessary information? Are the procedures used consistently within the organization when determining access of related workforce job functions? NIST guidance describes this implementation specification as calling for regulated entities to implement appropriate screening of persons who would have access to ePHI, and a procedure for obtaining clearance from appropriate offices or workforce members where access is provided or terminated.[555]

We issued guidance in 2017 addressing termination procedures.[556] Data breaches caused by current and former workforce members are a recurring issue across many industries, including the health care industry. Effective identity and access management policies and controls are essential to reduce the risks posed by these types of insider threats. Identity and access management can include many processes, but, most commonly, it would include the processes by which appropriate access to data is granted and terminated by creating and managing user accounts. Ensuring that user accounts are terminated—and in a timely manner—so that former workforce members do not have access to data, is one important way identity and access management can help reduce risks posed by insider threats. Additionally, effective termination procedures also reduce the risk that inactive user accounts (*e.g.,* user accounts that are not being used or are inactive but are not fully terminated or disabled) could be used by a current or former workforce member with malicious motives to get access to ePHI. The Department's guidance also offers tips to prevent unauthorized access to PHI by former workforce members, such as having standard procedures of all action items to be completed when an individual leaves.[557]

Guidance that we issued in 2019 further explains that ''security is a dynamic process.'' [558] Good security practices entail continuous awareness, assessment, and action in the face of changing circumstances. The information users can and should be allowed to access may change over time; organizations should recognize this in their policies and procedures and in their implementation of those policies and procedures. For example, if a user is promoted, demoted, or transfers to a different department, a user's need to access data may change. In such situations, the user's data access privileges should be re-evaluated and, as needed, modified to match the new role, if needed.[559] As described in other HHS guidance, these procedures should also address the complexity of the organization and the sophistication of its relevant electronic information systems.[560]

NIST guidance provides additional descriptions of key activities and sample questions for regulated entities to consider when implementing this standard and associated implementation specifications.[561] Regulated entities should establish a standard set of procedures that should be followed to recover access control devices (*e.g.,* identification badges, keys, access cards) when employment ends and, likewise, they should timely deactivate computer access (*e.g.,* disable user IDs and passwords) and facility access (*e.g.,* change facility security codes/PINs). Sample questions for implementation include the following: 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)? Is there a standard checklist for all action items that should be completed when a workforce member leaves (*e.g.,* return of all access devices, deactivation of accounts, and delivery of any needed data solely under the workforce member's control)? Do other organizations need to be notified to deactivate accounts to which that the workforce member had access in the performance of their employment duties?

However, regulated entities often do not establish or implement written procedures, nor, even in instances where they have established or implemented them, have they done so in an appropriate fashion to protect ePHI from improper access by current or former workforce members.

Consistent with the guidance described above and other proposals in this NPRM, the Department proposes to redesignate the workforce security standard at 45 CFR 164.308(a)(3)(i) as proposed 45 CFR 164.308(a)(9)(i), to add a paragraph heading to clarify the organization of the regulatory text, and to modify the regulatory text clarify that a regulated entity must implement written policies and procedures ensuring that workforce members have appropriate access to ePHI and to relevant electronic information systems. The regulated entity must also implement written policies and procedures preventing workforce members from accessing ePHI and relevant electronic information systems if they are not authorized to do so. The modifications we propose to the implementation specification for authorization and/or supervision would clarify that a regulated entity is required to establish and implement written procedures for the authorization and/or supervision of workforce members who access ePHI or relevant electronic information systems or who work in facilities where ePHI or relevant electronic information systems might be accessed.[562] We propose similar modifications to the implementation specification for workforce clearance procedure, which would require a regulated entity to establish and implement written procedures to determine that the access of a workforce member to ePHI or relevant electronic information systems is appropriate, in accordance with written policies and procedures for granting and revising access to ePHI and relevant electronic information systems as required by proposed 45 CFR 164.308(a)(10)(ii)(B).[563] Additionally, we propose several clarifications to the implementation specification for termination procedures. Specifically, the proposed implementation specification for modification and termination procedures at proposed 45 CFR 164.308(a)(9)(ii)(C) would require procedures for terminating a workforce member's access to ePHI and relevant electronic information systems, and to facilities where ePHI or relevant electronic information systems might be accessed. Proposed paragraph (a)(9)(ii)(C)(*1*) would require a regulated entity to establish and implement written procedures for terminating a workforce member's access to ePHI and relevant electronic information systems,

[555] *See* ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' *supra* note 461, p. 37.

[556] *See* ''Insider Threats and Termination Procedures,'' Cybersecurity Newsletter, Office for Civil Rights, U.S. Department of Health and Human Services (Nov. 2017), *https://www.hhs.gov/sites/default/files/november-cybersecurity-newsletter-11292017.pdf.*

[557] *See* ''Managing Malicious Insider Threats,'' *supra* note 528.

[558] *Id.*

[559] *See* 45 CFR 164.308(a)(4)(ii)(C).

[560] *See* ''Security Standards: Administrative Safeguards,'' *supra* note 517, p. 10–11.

[561] *See* ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' *supra* note 461.

[562] *See* proposed 45 CFR 164.308(a)(9)(ii)(A).

[563] *See* proposed 45 CFR 164.308(a)(9)(ii)(B).

and to locations where ePHI or relevant electronic information systems might be accessed. Proposed paragraph (a)(9)(ii)(C)(*2*) would require that the workforce member's access be terminated as soon as possible, but no later than one hour after the workforce member's employment or other arrangement ends. A proposed implementation specification for notification at proposed 45 CFR 164.308(a)(9)(ii)(D) would require a regulated entity to establish and implement written procedures for notifying another regulated entity of a change in, or termination of, a workforce member's authorization to access ePHI or relevant electronic information systems. Proposed paragraph (a)(9)(ii)(D)(*1*) would require the regulated entity to establish and implement written procedures for notifying another regulated entity after a change in or termination of a workforce member's authorization to access ePHI or relevant electronic information systems that are maintained by such other regulated entity where the workforce member is or was authorized to access such ePHI or relevant electronic information systems by the regulated entity making the notification. Proposed paragraph (a)(9)(ii)(D)(*2*) would require the notice to be provided as soon as possible, but no later than 24 hours after the workforce member's authorization to access ePHI or relevant electronic information systems is changed or terminated. Finally, a proposed new implementation specification for maintenance at proposed 45 CFR 164.308(a)(9)(ii)(E) would require a regulated entity to review and test its written workforce security policies and procedures at least once every 12 months and to modify them as reasonable and appropriate.[564] The proposed implementation specifications for termination procedures and notification implementation align with the Department's essential CPG for Revoke Credentials for Departing Workforce Members, Including Employees, Contractors, Affiliates, and Volunteers by requiring a regulated entity to promptly remove access following a change in or termination of a user's authorization to access ePHI.[565]

l. Section 164.308(a)(10)(i)—Standard: Information Access Management

The purpose of the standard for information access management is to protect ePHI by reducing the risk that other persons or technology assets may access the information for their own reasons. Existing HHS guidance explains that restricting access to only those persons and entities with a need for access is a basic tenet of security.[566] By implementing this standard, the risk of inappropriate disclosure, alteration, or destruction of ePHI is minimized. A regulated entity must determine those persons and technology assets that need access to ePHI within its environment. The implementation specifications associated with the standard on information access management are closely related to those associated with the standard for workforce security.[567] Compliance with the proposed and existing standards for information access management should support a regulated entity's compliance with the Privacy Rule's minimum necessary requirements, which requires a regulated entity to evaluate its practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of PHI.[568]

OCR's enforcement experience demonstrates that many regulated entities have not adequately implemented this standard. Thus, we believe it is necessary to consider strengthening the requirement. For example, on one occasion, a large covered entity's failure to implement its written policies and procedures to ensure that employees only had access to ePHI that they had proper authorization or authority to access enabled an employee to access the ePHI of more than 24,000 individuals.[569] This failure also enabled other employees to inappropriately access the ePHI of a celebrity.[570]

To ensure that regulated entities implement recommendations and best practices for securing ePHI, we propose to require in the standard for information access management and associated implementation specifications that a regulated entity must establish and implement written policies and procedures for authorizing access to ePHI and relevant electronic information systems that are consistent with the Privacy Rule. The Department also proposes to redesignate the standard at 45 CFR 164.308(a)(4)(i) as proposed 45 CFR 164.308(a)(10)(i) and to add a paragraph heading to clarify the organization of the regulatory text. Additionally, the Department proposes to modify three of the associated existing implementation specifications and to add three new implementation specifications as follows.

Specifically, the Department proposes to redesignate the implementation specification for isolating health care clearinghouse functions as proposed 45 CFR 164.308(a)(10)(ii)(A) and to modify it to require a health care clearinghouse that is part of a larger organization to establish and implement written policies and procedures that protect the ePHI and relevant electronic information systems of the clearinghouse from unauthorized access by the larger organization.

The existing implementation specification for isolating health care clearinghouse functions only applies in the situation where a health care clearinghouse is part of a larger organization. This would remain true under the proposal to revise this implementation specification, if adopted. In these situations, the health care clearinghouse is responsible for protecting the ePHI that it is creating, receiving, maintaining, and transmitting. As discussed in NIST guidance, if a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the ePHI of the clearinghouse from unauthorized access by the larger organization.[571] This necessarily includes its relevant electronic information systems. First, the regulated entity must determine

[564] *See* proposed 45 CFR 164.308(a)(9)(ii)(E).

[565] ''Cybersecurity Performance Goals,'' *supra* note 18.

[566] *See* ''Security Standards: Administrative Safeguards,'' *supra* note 517, p.11.

[567] *See, e.g.,* Resolution Agreement, ''Banner Health,'' Office for Civil Rights, U.S. Department of Health and Human Services (Dec. 20, 2022), *https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/banner-health-ra-cap/index.html;* ''Montefiore Medical Center,'' *supra* note 248.

[568] *See* 45 CFR 164.502(b) and 164.514(d).

[569] *See* Press Release, ''OCR Imposes a $2.15 Million Civil Money Penalty against Jackson Health System for HIPAA Violation,'' U.S. Department of Health and Human Services (Oct. 19, 2019), *https://public3.pagefreezer.com/browse/HHS.gov/31-12-2020T08:51/https://www.hhs.gov/about/news/2019/10/23/ocr-imposes-a-2.15-million-civil-money-penalty-against-jhs-for-hipaa-violations.html; see also* Notice of Proposed Determination, ''Jackson Health System,'' Office for Civil Rights, U.S. Department of Health and Human Services (July 22, 2019), *https://public3.pagefreezer.com/browse/HHS.gov/31-12-2020T08:51/https://www.hhs.gov/sites/default/files/jackson-health-system-notice-of-final-determination_508.pdf;* Notice of Final Determination, ''Jackson Health System,'' Office for Civil Rights, U.S. Department of Health and Human Services (Oct. 15, 2019), *https://public3.pagefreezer.com/browse/HHS.gov/31-12-2020T08:51/https://www.hhs.gov/sites/default/files/jackson-health-system-notice-of-final-determination_508.pdf.*

[570] *See* Press Release, ''HHS Office for Civil Rights Settles HIPAA Investigation with Arizona Hospital System Following Cybersecurity Hacking,'' U.S. Department of Health and Human Services (Feb. 2, 2023), *https://www.hhs.gov/about/news/2023/02/02/hhs-office-for-civil-rights-settles-hipaa-investigation-with-arizona-hospital-system.html.*

[571] *See* ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' *supra* note 461.

whether any of its components constitute a health care clearinghouse under the Security Rule.[572] If no health care clearinghouse functions exist within the organization, the regulated entity should document this finding. If a health care clearinghouse does exist within the organization, the regulated entity must implement procedures that are consistent with the Privacy Rule.[573] Questions for regulated entities to consider include: If health care clearinghouse functions are performed, are policies and procedures implemented to protect ePHI from the other functions of the larger organization? Does the health care clearinghouse share hardware or software with a larger organization of which it is a part? Does the health care clearinghouse share staff or physical space with staff from a larger organization? Has a separate network or subsystem been established for the health care clearinghouse, if reasonable and appropriate? Has staff of the health care clearinghouse been trained to safeguard ePHI from disclosure to the larger organization, if required for compliance with the Privacy Rule? [574] Regulated entities should also consider whether additional technical safeguards are needed to separate ePHI in electronic information systems used by the health care clearinghouse to protect against unauthorized access by the larger organization.

We also propose to redesignate the implementation specification for access authorization as proposed 45 CFR 164.308(a)(10)(ii)(B) and to modify it to emphasize that a regulated entity must establish and implement written policies and procedures for granting and revising access to ePHI and the regulated entity's relevant electronic information systems as necessary and appropriate for each prospective user and technology asset to carry out their assigned function(s) (*i.e.,* role-based access policies). Additionally, we propose to redesignate the implementation specification for access establishment and modification as 45 CFR 164.308(a)(10)(ii)(D) and to modify the heading to ''Access determination and modification.'' We also propose to modify this implementation specification to require a regulated entity to establish and implement written policies and procedures that, based on its access authorization policies, establish, document, review, and modify the access of each user and technology asset to specific components of the regulated entity's relevant electronic information systems. Such written policies and procedures would be required to be based upon the regulated entity's policies for authorizing access. Under this proposal, and consistent with the existing implementation specification,[575] the regulated entity would be required to establish standards for granting access to ePHI and relevant electronic information systems and provide formal authorization from the appropriate authority before granting access to ePHI or relevant electronic information systems. Regulated entities should regularly review personnel access to ePHI and relevant electronic information systems to ensure that access is still authorized and needed, and modify personnel access to ePHI and electronic information systems, as needed, based on review activities.

The existing implementation specification for access authorization calls for the regulated entity to implement policies and procedures for granting access to ePHI, for example, through components of its information system.[576] The Department's proposal to revise this implementation specification would provide greater specificity than our existing requirements, and echo NIST guidance on this topic. Specifically, NIST guidance [577] describes the key steps for developing policies and procedures for granting access to ePHI as follows:

- Decide and document procedures for how access to ePHI would 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 would be granted for privileged functions.
- Ensure that there is a list of personnel with authority to approve user requests to access ePHI and systems with ePHI.
- Identify authorized users with access to ePHI, including data owners and data custodians.
- Consider whether multiple access control methods are needed to protect ePHI according to the results of the risk assessment.
- Determine whether direct access to ePHI would ever be appropriate for individuals external to the organization (*e.g.,* business partners or patients seeking access to their own ePHI).

Other questions that a regulated entity should consider when establishing such policies and procedures include: Have appropriate authorization and clearance procedures, as specified in the standard for workforce security,[578] been performed prior to granting access? Do the organization's systems have the capacity to set access controls? Are there additional access control requirements for users who would be accessing privileged functions? Have organizational personnel been explicitly authorized to approve user requests to access ePHI and/or systems with ePHI?

The Department proposes three additional implementation specifications for authentication management, maintenance, and network segmentation. These specifications clarify the Department's expectations for compliance and are consistent with NIST guidance. We believe that the proposed additions would assist regulated entities in their efforts to prevent or mitigate attacks by malicious internal and external actors. For the implementation specification on authentication management at proposed 45 CFR 164.308(a)(10)(ii)(C), we propose to require a regulated entity to establish and implement written policies and procedures for verifying the identities of users and technology assets before accessing the regulated entity's relevant electronic information systems, including written policies and procedures for implementing MFA technical controls.[579] The proposed implementation specification for network segmentation at proposed 45 CFR 164.308(a)(10)(ii)(E) would require a regulated entity to establish and implement written policies and procedures that ensure that its relevant electronic information systems are segmented to limit access to ePHI to authorized workstations.

Finally, to address the Department's general concerns regarding the ongoing failure of many regulated entities to regularly review and revise their policies and procedures, the proposed implementation specification for maintenance at proposed 45 CFR

[572] 45 CFR 160.103 (definition of ''Health care clearinghouse'').

[573] 45 CFR 164.500(b); *see also* ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' *supra* note 461, p. 38.

[574] *See* ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' *supra* note 461, p. 38.

[575] 45 CFR 164.308(a)(4)(ii)(C).

[576] 45 CFR 164.308(a)(4)(ii)(B).

[577] *See* ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' *supra* note 461.

[578] *See* 45 CFR 164.308(a)(3); proposed 45 CFR 164.308(a)(9)(i).

[579] *See* proposed 45 CFR 164.312(f)(2)(ii) through (iv).

164.308(a)(10)(ii)(F) would require a regulated entity to review the written policies and procedures required by this standard at least once every 12 months and to modify them as reasonable and appropriate.

m. Section 164.308(a)(11)(i)—Standard: Security Awareness Training

A covered entity's workforce is its frontline not only in patient care and patient service, but also in safeguarding the privacy and security of PHI.[580] The health care sector's risk landscape continues to grow with the increasing number of interconnected, smart devices of all types, the increased use of interconnected medical record and billing systems, and the increased use of applications and cloud computing. This standard reflects the fact that training on data security for workforce members is essential for protecting an organization against cyberattacks.

An organization's training program should be an ongoing, evolving process and flexible enough to educate workforce members on new cybersecurity threats and how to respond to them. As such, regulated entities should consider how often to train workforce members on security issues, given the risks and threats to their enterprises, and how often to send security updates to their workforce members. Many regulated entities have determined that twice-annual training and monthly security updates are necessary, given their risks analyses.

Regulated entities should apply security updates and reminders to quickly communicate new and emerging cybersecurity threats to workforce members such as new social engineering ploys (*e.g.,* fake tech support requests and new phishing scams) and malicious software attacks including new ransomware variants. Entities need to address what type of training to provide to workforce members on security issues, given the risks and threats to their enterprises. Computer-based training, classroom training, monthly newsletters, posters, email alerts, and team discussions are all tools that different organizations use to fulfill their training requirements. Entities must also address how to document that training to workforce members was provided, including dates and types of training, training materials, and evidence of workforce participation.

HHS has issued many types of training materials on securing PHI.[581] NIST has also provided detailed guidance for developing and implementing workforce training programs.[582] Despite this existing guidance, regulated entities often fail to provide appropriate training to adequately safeguard ePHI. For example, in one investigation, OCR investigators found evidence that not only had an ambulance company potentially failed to conduct a risk analysis, it also potentially failed to implement a security training program or to train any of its employees.[583] Such failures can contribute to breaches of individuals' unsecured ePHI.

To ensure security awareness training compliance, a regulated entity needs to regularly educate its workforce members on the evolving technological threats to ePHI, how to use the technology that the regulated entity has adopted and implemented, and the specific procedures workforce members must follow to ensure that the ePHI remains protected. Additionally, while many educational programs for clinicians provide general training on the HIPAA Rules, the curriculums vary widely. Without providing its own training on the Security Rule, a regulated entity cannot ensure that the training its workforce received elsewhere meets the required standards.

Given the failure of regulated entities to implement the security awareness and training standard and consistent with existing guidance, the Department proposes to provide more detailed requirements for security awareness training. Specifically, the Department proposes to rename and redesignate the standard for security awareness and training at 45 CFR 164.308(a)(5)(i) as the standard for security awareness training at proposed 45 CFR 164.308(a)(11)(i) and to add a paragraph heading to clarify the organization of the regulatory text. The proposed standard would require a regulated entity to implement security awareness training for all workforce members on protection of ePHI and information systems as necessary and appropriate for the members of the workforce to carry out their assigned function(s) (*i.e.,* role-based training). The proposals to revise this standard would also align with the Department's essential CPG for Basic Cybersecurity Training because they would require a regulated entity to educate users on how to access ePHI and electronic information systems in a manner that protects the confidentiality, integrity, and availability of ePHI.[584] Additionally, the proposals would align with the essential CPG for Email Security by requiring a regulated entity to train workforce members to guard against, detect, and report suspected or known security incidents, including, but not limited to, malicious software and social engineering.[585]

We propose four implementation specifications for the proposed security awareness training standard. The proposed implementation specification for training at 45 CFR 164.308(a)(11)(ii)(A) would require a regulated entity to establish and implement security awareness training for all workforce members that addresses the following:

- The written policies and procedures required by the Security Rule, as necessary and appropriate for the workforce members to carry out their assigned functions.[586]
- Guarding against, detecting, and reporting suspected or known security incidents, including but not limited to malicious software and social engineering.[587]
- The written policies and procedures for accessing the regulated entity's electronic information systems, including, but not limited to, safeguarding passwords, setting unique passwords of sufficient strength to ensure the confidentiality, integrity, and availability of ePHI, and establishing limitations on sharing passwords. Consistent with the recommendation from NCVHS, such policies and procedures should ensure that the regulated entity does not employ default passwords and should prevent workforce members from sharing of credentials.[588] We do not propose that passwords be required to meet a particular standard because best practices for password configuration may change over time; however, we believe that it is essential for a regulated

[580] *See* ''Train Your Workforce, so They Don't Get Caught by a Phish!,'' Cybersecurity Newsletter, Office for Civil Rights, U.S. Department of Health and Human Services (July 2017), *https://www.hhs.gov/sites/default/files/july-2017-ocr-cyber-newsletter.pdf.*

[581] *See* ''Training Materials,'' Office for Civil Rights, U.S. Department of Health and Human Services, *https://www.hhs.gov/hipaa/for-professionals/training/index.html.*

[582] *See* ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' *supra* note 461.

[583] *See* Resolution Agreement, ''West Georgia Ambulance, Inc.'' Office for Civil Rights, U.S. Department of Health and Human Services (Dec. 23, 2019), *https://www.hhs.gov/sites/default/files/west-georgia-ra-cap.pdf.*

[584] ''Cybersecurity Performance Goals,'' *supra* note 18.

[585] *Id.*

[586] Proposed 45 CFR 164.308(a)(11)(ii)(A)(*1*).

[587] Proposed 45 CFR 164.308(a)(11)(ii)(A)(*2*).

[588] Proposed 45 CFR 164.308(a)(11)(ii)(A)(*3*); Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 1; Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123, p. 6–7.

entity to educate its workforce members on best practices for setting passwords and to ensure that its workforce members implement such best practices.

The Department proposes to replace the implementation specification for periodic security updates [589] with one addressing the timing and frequency of security awareness training at proposed 45 CFR 164.308(a)(11)(ii)(B). Specifically, we propose to require a regulated entity to provide such training to each member of the regulated entity's workforce by the compliance date for this rulemaking, if finalized, and at least once every 12 months thereafter.[590] For example, under this proposal, workforce members would receive security awareness training on the protection of ePHI and on the regulated entity's Security Rule policies and procedures that is based on their specific role at least once a year. A regulated entity would be required to provide role-based security awareness training to a new workforce member within a reasonable period of time, but no later than 30 days after the workforce member first has access to the regulated entity's relevant electronic information systems.[591] We also propose to require that the regulated entity provide such training.[592] For example, if the entity implements a new EHR system, it would be required to also train its workforce, as appropriate, on measures to guard against security incidents related to the installation, maintenance and/or use of the system.

Additionally, the Department proposes at proposed 45 CFR 164.308(a)(11)(ii)(C) an implementation specification for ongoing education. This would require a regulated entity to provide its workforce members with ongoing reminders of their security responsibilities and notice of relevant threats, including but not limited to, new and emerging malicious software and social engineering. Lastly, we propose a new implementation specification for documentation at proposed 45 CFR 164.308(a)(11)(ii)(D) that would require a regulated entity to document that it has provided training and ongoing reminders to its workforce members.

n. Section 164.308(a)(12)(i)—Standard: Security Incident Procedures

Addressing security incidents is an integral part of an overall security program. While a regulated entity will never be able to prevent all security incidents, implementing the Security Rule standards would reduce the amount and negative consequences of security incidents it encounters. Even regulated entities with detailed security policies and procedures and advanced technology may experience security incidents, but through sufficient planning and continued monitoring generally can mitigate the negative effects of such incidents on regulated entities, and, ultimately, individuals. The security incident procedures standard is intended to help ensure that a regulated entity conducts such planning and monitoring to allow it to mitigate such negative effects.

The Department has also provided guidance that a regulated entity can use to devise its security incident plans. The policies and procedures a regulated entity establishes to prepare for and respond to security incidents can pay dividends with faster recovery times and reduced compromises of ePHI.[593] A well thought-out, well-tested security incident response plan is integral to ensuring the confidentiality, integrity, and availability of a regulated entity's ePHI. A timely response to a security incident can be one of the best ways to prevent, mitigate, and recover from future cyberattacks. For example, responding to a single intrusion or inappropriate access can prevent a pattern of repeated malicious actions. It is extremely important that a regulated entity analyzes an incident to establish what has occurred and its root cause. Doing so will enable the regulated entity to use that information to update its security incident response plans. The Department has previously issued guidance addressing such activities as forming a security incident response team, identifying and responding to security incidents, mitigating harmful effects of and documenting a security incident, and breach reporting.[594]

NIST also offers guidance for addressing security incidents.[595] It describes four key activities with detailed descriptions and sample questions:

- Determine the goals of an incident response.
- Develop and deploy an incident response team or other reasonable and appropriate response mechanism.
- Develop and implement policy and procedures to respond to and report security incidents.
- Incorporate post-incident analysis into updates and revisions.

NIST has also issued comprehensive guidelines for incident handling, particularly for analyzing incident related data and determining the appropriate response to each incident.[596] For example, the NIST Cybersecurity Framework addresses these activities as part of the core function of ''[respond—a]ctions regarding a detected cybersecurity incident are taken.'' [597] ''Respond'' supports the ability of the regulated entity ''to contain the effects of cybersecurity incidents. Outcomes within this Function [include] incident management, analysis, mitigation, reporting, and communication.'' [598]

Despite this existing guidance, OCR's enforcement experience indicates that many regulated entities have not met the existing standard, so we believe that additional specificity regarding their obligations and liability for incident response is warranted. Accordingly, the Department proposes to redesignate the standard for security incident procedures as 45 CFR 164.308(a)(12)(i), to add a paragraph heading to clarify the organization of the regulatory text, and to modify the regulatory text to clarify that a regulated entity would be required to implement written policies and procedures to ''respond to,'' rather than ''address,'' security incidents. Additionally, we propose to clarify expectations by adding an implementation specification for planning and testing at proposed 45 CFR 164.308(a)(12)(ii)(A)(*1*) that would require a regulated entity to establish written security incident response plan(s) and procedures documenting how workforce members are to report suspected or known security incidents and how the regulated entity will respond to suspected or known security incidents.[599]

Internal reporting is an essential component of security incident procedures.[600] Plans and procedures for

[589] 45 CFR 164.308(a)(5)(ii)(A).

[590] Proposed 45 CFR 164.308(a)(11)(ii)(B)(*1*).

[591] Proposed 45 CFR 164.308(a)(11)(ii)(B)(*2*).

[592] Proposed 45 CFR 164.308(a)(11)(ii)(B)(*3*).

[593] *See* ''HIPAA Security Rule Security Incident Procedures,'' Cybersecurity Newsletter, Office for Civil Rights U.S. Department of Health and Human Services (Oct. 2022), *https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-october-2022/index.html.*

[594] *Id.*

[595] *See* ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' *supra* note 461.

[596] *See* Paul Cichonski, et al., ''Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology,'' NIST Special Publication 800–61, Revision 2, National Institute of Standards and Technology, U.S. Department of Commerce (Aug. 2012), *https://www.nist.gov/privacy-framework/nist-sp-800-61.*

[597] ''The NIST Cybersecurity Framework (CSF) 2.0,'' (removed emphasis on ''Actions regarding a detected cybersecurity incident are taken'' in original), *supra* note 15, p. 9.

[598] *Id.*

[599] Proposed 45 CFR 164.308(a)(12)(ii)(A)(*1*).

[600] *See, e.g.,* Joint Task Force, ''Security and Privacy Controls for Information Systems and

Continued

reporting of suspected or known security incidents may address to whom, when, and how such incidents are to be reported. The recipient(s) and the content of such reports, according to such plans and procedures, may vary based on the type of incident and the role of the workforce member making the report. We do not propose to dictate the form, format, or content of such report. Rather, we believe that regulated entities would be best situated to identify the point(s) of contact for their organization (*e.g.,* Chief Information Security Officer, IT security team, business associate engaged to support incident response activities for the regulated entity) for such reports and the type of information they need to determine how to respond to the suspected or known security incident.

The proposal to require a regulated entity to establish written security incident response plans and procedures for how it will respond to suspected or known security incidents would align with the enhanced CPG for Third Party Incident Reporting because it would address the procedures for how and when a business associate would report to a covered entity or another business associate known or suspected security incidents, as required by proposed 45 CFR 164.314(a)(2)(i)(C).[601]

Under proposed 45 CFR 164.308(a)(12)(ii)(A)(*2*) and (*3*), the regulated entity would be required to implement written procedures for testing and revising the security incident response plan(s) and then, using those written procedures, review and test its security incident response plans at least once every 12 months and document the results of such tests. The regulated entity would also be required to modify the plan(s) and procedures as reasonable and appropriate, based on the results of such tests and the regulated entity's circumstances.

This proposal, if finalized, would include requirements that align with the Department's essential CPG for Basic Incident Planning and Preparedness to have effective responses to and recovery from security incidents.[602] It also aligns with the Department's enhanced CPG for Centralized Incident Planning and Preparedness by requiring a regulated entity to maintain, revise, and test security incident response plans.[603]

Additionally, the Department proposes to redesignate the implementation specification for response and reporting at 45 CFR 164.308(a)(6)(ii) as 45 CFR 164.308(a)(12)(ii)(B) and to rename it ''Response.'' We also propose to modify the existing implementation specification by separating it into two paragraphs: one at paragraph (a)(12)(ii)(B)(*1*) for identifying and responding to suspected or known security incidents, and the other at paragraph (a)(12)(ii)(B)(*2*) for mitigating, to the extent practicable, the harmful effects of suspected or known security incidents. The Department also proposes to add three additional paragraphs to this implementation specification. Proposed 45 CFR 164.308(a)(12)(ii)(B)(*3*) would require a regulated entity to identify and remediate, to the extent practicable, the root cause(s) of suspected or known security incidents, while proposed 45 CFR 164.308(a)(12)(ii)(B)(*4*) would require the regulated entity to eradicate the security incidents that are suspected or known to the regulated entity. We would expect eradication to include the removal of malicious software, inappropriate materials, and any other components of the incident from the regulated entity's relevant electronic information systems.[604] Finally, proposed 45 CFR 164.308(a)(12)(ii)(B)(*5*) would require a regulated entity to develop and maintain documentation of investigations, analyses, mitigation, and remediation for security incidents that are suspected or known. For example, verbal reports of a suspected or known security incident would be required to be documented in writing. Under proposed 45 CFR 164.316(b)(1), if finalized, a regulated entity would be required to maintain such documentation for six years from the date of its creation or the date when it last was in effect, whichever is later. These proposals are consistent with existing guidance described above and with other proposals or existing regulatory standards to secure health information.[605]

o. Section 164.308(a)(13)(i)—Standard: Contingency Plan

The purpose of any contingency plan is to allow an organization to return to its daily operations as quickly as possible after an unforeseen event.[606] The contingency plan protects resources, minimizes customer inconvenience, and identifies key staff, assigning specific responsibilities in the context of the recovery. Contingency plans are critical to protecting the availability, integrity, and security of data during unexpected adverse events. Contingency plans should consider not only how to respond to disasters such as fires and floods, but also how to respond to cyberattacks. Cyberattacks using malicious software, such as ransomware, may render an organization's data unreadable or unusable. In the event data is compromised by a cyberattack, restoring the data from backups may be the only option for recovering the data and restoring normal business operations. For example, the faulty software update by CrowdStrike made it impossible for health care systems worldwide to use their Windows-based systems.[607] There were many instances where surgical procedures and health care appointments were cancelled, schedules upended, and pharmacies were unable to fill prescriptions. Regulated entities need to make and implement contingency plans they would use when such events occur to enable themselves to get back to their core functions of providing or paying for health care.

The Department and NIST have issued extensive guidance on contingency planning, including detailed descriptions of key activities, sample questions for regulated entities to consider when standing up a contingency plan, and information on how the results of the risk analysis feed into contingency plans.[608] Unfortunately, many regulated entities have not implemented the required

Organizations,'' NIST Special Publication 800–53, Revision 5, National Institute of Standards and Technology, U.S. Department of Commerce, p. 157 (Sept. 2020), *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.*

[601] ''Cybersecurity Performance Goals,'' *supra* note 18; *see also* proposed 45 CFR 164.314(a)(2)(i)(C).

[602] ''Cybersecurity Performance Goals,'' *supra* note 18.

[603] *Id.*

[604] *See* ''Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology,'' *supra* note 597.

[605] *See, e.g.,* ''New York State Register,'' *supra* note 14; ''Invitation for Preliminary Comments on Proposed Rulemaking: Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking,'' *supra* note 14; *see also* Cal. Civ. Code Section 1798.185.

[606] *See* ''Plan A. . .B. . .Contingency Plan!'' Cybersecurity Newsletter, Office for Civil Rights, U.S. Department of Health and Human Services (Mar. 2018), *https://www.hhs.gov/sites/default/files/march-2018-ocr-cyber-newsletter-contingency-planning.pdf.*

[607] *See* Kate Conger, et al., ''What Is Crowdstrike?,'' New York Times (July 19, 2024), *https://www.nytimes.com/2024/07/19/business/what-is-crowdstrike.html?searchResultPosition=2; see also* ''Remediation and Guidance Hub: Falcon Content Update for Windows Hosts,'' (July 31, 2024), *https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/.*

[608] *See* ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' *supra* note 461; *see also* ''Security Standards: Administrative Safeguards,'' *supra* note 517, p. 19–22.

planning and then have been unable to fully recover from ransomware attacks that bring down electronic systems that create, receive, maintain, or transmit ePHI. For example, a large health system that experienced a ransomware attack had to shut down services at multiple locations and encountered difficulties restoring those services. OCR's investigation indicated a potential failure to, among other things, implement contingency plans.[609] Such planning is crucial for maintaining the resilience of a regulated entity's health IT.

To address these inadequacies in compliance and to protect the confidentiality, integrity, and availability of ePHI, the Department proposes to redesignate the standard for a contingency plan at 45 CFR 164.308(a)(7)(i) as proposed 45 CFR 164.308(a)(13)(i), to add a paragraph heading to clarify the organization of the regulatory text, and to modify the regulatory text to clarify it. The modified standard, as proposed, would require a regulated entity to establish (and implement as needed) a written contingency plan, consisting of written policies and procedures for responding to an emergency or other occurrence, including, but not limited to, fire, vandalism, system failure, natural disaster, or security incident, that adversely affects relevant electronic information systems.

The Department proposes a new implementation specification for criticality analysis at proposed 45 CFR 164.308(a)(13)(ii)(A). This would require a regulated entity to perform and document an assessment of the relative criticality of its relevant electronic information systems and technology assets in its relevant electronic information systems. The proposal would not limit this analysis to electronic information systems that create, receive, maintain, or transmit ePHI because other electronic information systems and/or technology assets may be crucial to ensuring the confidentiality, integrity, or availability of ePHI, providing patient care, and supporting other business needs. A prioritized list of specific relevant electronic information systems and technology assets in those electronic information systems would help a regulated entity to determine their criticality and the order of restoration.[610]

Under this proposal, the implementation specification for establishing and implementing a data backup plan would be redesignated as proposed 45 CFR 164.308(a)(13)(ii)(B) and renamed ''Data backups.'' It would also be modified to clarify that the procedures to create and maintain exact retrievable copies of ePHI must be in writing, and to also require such procedures to include verifying that the ePHI has been copied accurately. For example, the ability to access ePHI from a remote location in the event of a total failure should be reflected in the procedures specified for data backups.

The proposed implementation specification for backing up information systems at proposed paragraph (a)(13)(ii)(C) would require a regulated entity to establish and implement written procedures to create and maintain backups of its relevant electronic information systems, including verifying the success of such backups. Establishing such procedures would ensure that the ePHI in relevant electronic information systems is both protected and available.

Additionally, the Department proposes to redesignate the implementation specification for disaster recovering planning as paragraph (a)(13)(ii)(D). We propose to clarify that a regulated entity would be required to establish (and implement as needed) written procedures to restore both its critical relevant electronic information systems and data within 72 hours of the loss, and to restore the loss of other relevant electronic information systems and data in accordance with its criticality analysis.[611]

The Department proposes to clarify the implementation specification for emergency mode operation planning, redesignated as proposed 45 CFR 164.308(a)(13)(ii)(E), by clarifying that procedures must be written. We also propose to redesignate the implementation specification for testing and revision procedures as paragraph (a)(13)(ii)(F) and to clarify that procedures for testing and revising of the required contingency plans must be established in writing. We propose to require a regulated entity to review and implement its procedures for testing contingency plans at least once every 12 months, to document the results of such tests, and to modify those plans as reasonable and appropriate based on the results of those tests.

p. Section 164.308(a)(14)—Standard: Compliance Audit

The final standard we propose under 45 CFR 164.308(a) is a new standard for compliance audits at proposed 45 CFR 164.308(a)(14). For this proposed standard, the Department proposes to require regulated entities to perform and document an audit of their compliance with each standard and implementation specification of the Security Rule at least once every 12 months.

While the Security Rule does not currently require regulated entities to conduct internal or third-party compliance audits, such activities are important components of a robust cybersecurity program. The Government Accountability Office has published guidance on conducting cybersecurity performance audits for Federal agencies.[612] Audits are typically conducted independently from information security management, and the function generally reports to the governing body of the regulated entity. This independence can provide an objective view of the regulated entity's policies and practices. According to the Institute of Internal Auditors, an internal audit provides ''[i]ndependent and objective assurance and advice on all matters related to the achievement of objectives.'' [613] An internal audit may be conducted by a business associate of a covered entity or a subcontractor of a business associate. These activities provide regulated entities with confidence in the effectiveness of their risk management plan. Thus, we believe that this proposal would aid a regulated entity in ensuring compliance with the Security Rule, and ultimately, protecting ePHI. We do not propose to specify whether the compliance audit should be performed by the regulated entity or an external party.[614]

[609] *See* Press Release, ''HHS Office for Civil Rights Settles HIPAA Security Rule Failures for $950,000,'' U.S. Department of Health and Human Services (July 1, 2024), *https://prod-wwwhhsgov.cloud.hhs.gov/about/news/2024/07/01/hhs-office-civil-rights-settles-hipaa-security-rule-failures-950000.html.*

[610] *See* ''Security Standards: Administrative Safeguards,'' *supra* note 517, p. 22.

[611] *See* proposed 45 CFR 164.308(a)(13)(ii)(A).

[612] *See* ''Cybersecurity Program Audit Guide,'' GAO–23–104705, U.S. Government Accountability Office, p. 1 (Sept. 28, 2023), *https://www.gao.gov/products/gao-23-104705; see also* ''Security and Privacy Controls for Information Systems and Organizations,'' *supra* note 600.

[613] *See* ''The IIA's Three Lines Model: An update of the Three Lines of Defense,'' The Institute of Internal Auditors, p. 4 (Sept. 9, 2020), *https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf.*

[614] We believe that health plans that are subject to HIPAA and to the Employee Retirement Income Security Act of 1974 could comply with the proposed compliance audit requirement and follow the Employee Benefits Security Administration's Cybersecurity Program Best Practices, which specifies that all such plans have a reliable annual third party audit of security controls. ''Cybersecurity Program Best Practices,'' Employee Benefits Security Administration, U.S. Department of Labor, p. 1, 2 (Apr. 2021), *https://www.dol.gov/*

Continued

q. Section 164.308(b)(1) and (2)—Standard: Business Associate Contracts and Other Arrangements

Vendor management and identification of risks in a supply chain are essential to controlling the introduction of new threats and risks to a regulated entity.[615] NIST guidance explains that regulated entities, are permitted to include more stringent cybersecurity measures in business associate agreements than those required by the Security Rule.[616] Such requirements would need to be agreed upon by both parties to the business associate agreement.[617] The guidance also recommends establishing a process for measuring contract performance and terminating the contract if security requirements are not being met. Important considerations include: 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 would such additional assurances be documented (*e.g.,* in the business associate agreement, service-level agreement, or other documentation) and how would they be met (*e.g.,* providing documentation of implemented safeguards, audits, certifications)?

The Security Rule requires a regulated entity to protect the confidentiality, integrity, and availability of all ePHI that it creates, receives, maintains, or transmits.[618] It also requires a regulated entity to obtain written satisfactory assurances that its business associate will appropriately safeguard ePHI before allowing the business associate to create, receive, maintain, or transmit ePHI on its behalf.[619] However, the Security Rule does not require a regulated entity to verify that entities that create, receive, maintain, or transmit ePHI on its behalf are in fact taking the necessary steps to protect such ePHI. The lack of such a requirement may leave a gap in protections from risks to ePHI related to regulated entities' vendors and supply chains. Accordingly, the Department proposes several modifications to the Security Rule to provide greater assurance that business associates and their subcontractors are protecting ePHI because a subcontractor to a business associate is also a business associate. The Department proposes to redesignate 45 CFR 164.308(b)(1) and (2) as proposed 45 CFR 164.308(b)(1)(i) and (ii), respectively. Additionally, we propose to make a technical correction to the standard for business associate contracts and other arrangements for organizational clarity, separating proposed paragraph (b)(1)(i) into paragraphs (b)(1)(i)(A) and (B). We believe this is a non-substantive change that would have no effects on any regulatory, recordkeeping, or reporting requirement, nor would it change the Department's interpretation of any regulation. We also propose to modify both to require a regulated entity to verify that the business associate has deployed the technical safeguards required by 45 CFR 164.312[620] in addition to obtaining satisfactory assurances that its business associate would comply with the Security Rule.[621] To assist regulated entities in complying with the new standard, we propose to redesignate the implementation specifications at 45 CFR 164.308(b)(3) as 45 CFR 164.308(b)(2) and propose to add an implementation specification for written verification at proposed 45 CFR 164.308(b)(2)(ii) that would require the regulated entity to obtain written verification from the business associate that the business associate has deployed the required technical safeguards.[622] The Department proposes to require that the regulated entity obtain this written verification documenting the business associate's deployment of the required technical safeguards at least once every 12 months.[623] Additionally, we propose that the verification include a written analysis of the business associate's relevant electronic information systems.[624] The written analysis would be required to be performed by a person with appropriate knowledge of and experience with generally accepted cybersecurity principles and methods for ensuring the confidentiality, integrity, and availability of ePHI to verify the business associate's compliance with each standard and implementation specification in 45 CFR 164.312.[625] We also propose to require that the written verification be accompanied by a written certification by a person who has the authority to act on behalf of the business associate that the analysis has been performed and is accurate.[626] The proposal would permit the parties to determine the appropriate person to perform the analysis and how that person is engaged or compensated. This person may be a member of the covered entity's or business associate's workforce or an external party.

This proposed new requirement that a regulated entity obtain written verification from its business associates that they have deployed technical safeguards combined with the existing requirement to obtain written satisfactory assurances that they safeguard ePHI, aligns with the Department's essential CPG for Vendor/Supplier Cybersecurity Requirements.[627] This CPG calls for regulated entities to identify, assess, and mitigate risks to ePHI used by or disclosed to business associates.[628]

r. Section 164.308(b)(3)—Standard: Delegation To Business Associate

Based on the OCR's investigations and enforcement experience, we believe that some regulated entities are not aware that they retain compliance responsibility for implementing requirements of the Security Rule, even when they have delegated the functions of designated security official to a business associate. Therefore, the Department proposes a new standard for delegation to a business associate at proposed 45 CFR 164.308(b)(3). The proposed standard would clarify that a regulated entity may permit a business associate to serve as its designated security official.[629] However, a regulated entity that delegates actions, activities, or assessments required by the Security Rule to a business associate remains liable for compliance with all the applicable provisions of the Security Rule.[630]

4. Request for Comment

The Department requests comment on the foregoing proposals, including any benefits, drawbacks, or unintended consequences. We also request comment on the following considerations in particular. For any proposed timeframe that a commenter believes is not appropriate, we request comment and explanation on a more appropriate timeframe.

sites/dolgov/files/ebsa/pdf_files/best-practices.pdf; ''Cybersecurity Guidance Update,'' Employee Benefits Security Administration, U.S. Department of Labor (Sept. 6, 2024), *https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity/compliance-assistance-release-2024-01.*

[615] *See* ''Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,'' *supra* note 461.

[616] *Id.* at 54.

[617] *Id.*

[618] *See* 45 CFR 164.306(a)(1).

[619] *See* 45 CFR 164.308(b).

[620] *See* proposed 45 CFR 164.308(b)(1)(i) and (ii).

[621] *Id.*

[622] *See* proposed 45 CFR 164.308(b)(2)(ii).

[623] *Id.*

[624] Proposed 45 CFR 164.308(b)(2)(ii)(A).

[625] *Id.*

[626] Proposed 45 CFR 164.308(b)(2)(ii)(B).

[627] ''Cybersecurity Performance Goals,'' *supra* note 18; *see also* proposed 45 CFR 164.308(b)(2)(i).

[628] ''Cybersecurity Performance Goals,'' *supra* note 18.

[629] Proposed 45 CFR 164.308(b)(3)(i).

[630] Proposed 45 CFR 164.308(b)(3)(ii).

a. Whether the Department should require a regulated entity to implement any additional administrative safeguards. If so, please explain.

b. Whether the Department should not require a regulated entity to implement any of the existing or proposed standards for implementation specifications. If so, please explain.

c. Whether there are additional implementation specifications that should be adopted for any of the standards for administrative safeguards.

d. Whether the Department should provide any exceptions to the administrative safeguards or related implementation specifications. If so, please explain when and why any exceptions should apply.

e. Whether once every 12 months is the appropriate frequency between reviews of policies, procedures, and other activities required by the other standards for administrative safeguards.

f. Whether there are any special considerations for business associates and business associate agreements that the Department should be aware of with respect to administrative safeguards.

g. Whether there are any requirements for business associates and business associate agreements that the Department should include in administrative safeguards that it did not propose.

h. Whether the Department should require covered entities to report to their business associates (or business associates to their subcontractors) the activation of the covered entities' (or business associates') contingency plans. If so, please explain the appropriate circumstances of and the appropriate amount of time for such notification.

i. Whether once every 12 months is an appropriate length of time in which a covered entity must verify and document that a business associate has deployed technical safeguards pursuant to the requirements.

j. Whether the Department should require covered entities to obtain satisfactory assurances and verify that a business associate has implemented physical or other safeguards in addition to deploying technical safeguards before permitting it to create, receive, maintain, or transmit ePHI on its behalf.

k. Whether on an ongoing basis, but at least once every 12 months and when there is a change to a regulated entity's environment or operations that affects ePHI, is the appropriate frequency for updating the technology asset inventory and network map?

l. Whether on an ongoing basis, but at least once every 12 months and when there is a change to the regulated entity's environment or operations that affects ePHI, is the appropriate frequency for performing a risk analysis?

m. Whether there are additional events for which the Department should require a regulated entity to update its risk analysis. If so, please explain.

n. Whether the Department should include or exclude any specific circumstances from its explanation of environmental or operational changes when determining whether review or update of the written inventory of technology assets and network map or review of the risk analysis written assessment is warranted.

o. Whether the proposed requirement in the standard for evaluation, to perform a written technical and nontechnical evaluation within a reasonable period of time before making a change in the regulated entity's environment or operations pursuant to the requirements, is sufficiently clear. If not, how should the Department clarify it? For example, should the Department require a specific amount of time, and if so, what length of time?

p. Whether at least once every 12 months is the appropriate frequency for reviewing and updating written policies and procedures for patch management, sanctions policies and procedures information system activity review, workforce security, and information access management.

q. Whether as reasonable and appropriate in response to changes in the risk analysis, but at least once every 12 months, is the appropriate frequency for reviews of a regulated entity's written risk management plan.

r. Whether the proposed frequency for security awareness training is appropriate.

s. Whether the proposed substance of the security awareness training is appropriate, and any recommendations for additional required content.

t. Whether the proposed timelines for applying patches, updates, and upgrades are appropriate.

u. Whether the Department should set a time limit for applying patches, updates, and upgrades to configurations of relevant electronic information systems to address moderate and low risks. If so, please explain and provide a recommendation.

v. Whether the amount of time regulated entities currently retain records of information system activity varies by the type of record, and for how long such records are retained.

w. Whether the Department should specify the length of time for which records of information system activity should be retained. If so, please explain.

x. Whether the Department should require that a regulated entity notify other regulated entities of the termination of a workforce member's access to ePHI in less than 24 hours after the workforce member's termination. If so, please explain what would be an appropriate period of time (*e.g.,* three business hours, 12 hours).

y. Whether at least once every 12 months is the appropriate frequency for testing security incident response plans, documenting the results, and revising such plans.

z. Whether it is reasonable and appropriate to require that regulated entities restore loss of critical relevant electronic information systems and data in 72 hours or less.

aa. Whether the Department should require a regulated entity to restore all of its relevant electronic information systems and data within 72 hours?

bb. Whether the Department should require some regulated entities to restore their relevant electronic information systems and data in less than 72 hours? If so, please explain.

cc. Whether at least once every 12 months is the appropriate frequency for the testing of contingency plans?

dd. Whether annual auditing of a regulated entity's compliance with the Security Rule is appropriate.

ee. Whether the Department should specify the level of detail or standard required for the annual compliance audit. If so, please explain.

ff. Whether the Department should require a regulated entity to obtain written verification of their business associates' implementation of the administrative and physical safeguards that are required by the Security Rule, in addition to the proposed requirement to obtain verification of implementation of the technical safeguards. If so, please explain.

gg. Whether there are other requirements for which the Department should require that the person performing them have a specific level or type of expertise. If so, please explain.

E. Section 164.310—Physical Safeguards

1. Current Provisions

A person with physical access to electronic media or a regulated entity's electronic information systems that create, receive, maintain, or transmit or that otherwise affect the confidentiality, integrity, and availability of ePHI might have the opportunity to change the configurations of its relevant electronic information systems, install malicious software or otherwise adversely affect technology assets in its relevant

electronic information systems, change information, or access ePHI or other sensitive information.[631] Any of these actions has the potential to adversely affect the confidentiality, integrity, or availability of ePHI, which means that physical safeguards for electronic media and a regulated entity's relevant electronic information systems are critical to protecting the security of ePHI. Thus, the physical safeguards standards address the essential requirements for regulated entities to apply to limit physical access to their relevant electronic information systems to only authorized workforce members. As discussed above, ePHI is increasingly transmitted using interconnected systems that rely on cloud computing. The shift to a cloud-based infrastructure may increase regulated entities' reliance on business associates to maintain and access ePHI stored in the cloud.[632] Additionally, the shift to cloud computing enables regulated entities' workforce members to access ePHI and relevant electronic information systems from a greater number of locations. Accordingly, regulated entities must appropriately expand and/or ensure that applied physical safeguards take into account these new arrangements.

Section 164.310 includes the four standards with which a regulated entity must comply to physically secure relevant electronic information systems and the premises where they are located. These standards require regulated entities to implement physical safeguards for facility access controls, workstation use, workstation security, and device and media controls in a manner that conforms with 45 CFR 164.306(c), the general compliance provision for the security standards.

As discussed above in greater detail, physical safeguards encompass the physical measures, and related policies and procedures, to protect relevant electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion.[633] The standard for facility access controls applies to protect the physical premises, while the standards for workstation use, workstation security, and device and media controls are aimed at protecting the electronic information systems and electronic media that create, receive, maintain, or transmit ePHI or that otherwise affect its confidentiality, integrity, and availability.

The standard for facility access controls at 45 CFR 164.310(a)(1) requires a regulated entity to implement policies and procedures that limit physical access to electronic information systems and facilities that contain those systems. Section 164.310(a)(1) also requires a regulated entity to ensure its policies and procedures allow persons who are properly authorized to access its facilities.

Under 45 CFR 164.310(a)(2), a regulated entity must implement the standard for facility access controls in accordance with four implementation specifications. The implementation specification for contingency operations addresses the establishment (and implementation as needed) of procedures that allow for facility access in support of the restoration of lost data under a disaster recovery plan and emergency mode operations.[634] Section 164.310(a)(2)(ii) contains the specification for a facility security plan and addresses the implementation of policies and procedures to safeguard facilities and equipment in such facilities from unauthorized physical access, tampering, and theft. The implementation of procedures for role-based access control, including for visitors and for access to software programs for testing and revision is addressed in 45 CFR 164.310(a)(2)(iii), while 45 CFR 164.310(a)(2)(iv) addresses the implementation of policies and procedures for the documentation of repairs and modifications to physical security components of a facility, such as hardware, walls, doors, and locks.

Section 164.310(b) requires a regulated entity to implement policies and procedures specifying proper workstation functions, the manner in which those functions are to be performed, and the physical attributes of the environment for where specific workstations or classes of workstation used for accessing ePHI.[635] This standard is not accompanied by standalone implementation specifications, compared to the standards for facility access controls at 45 CFR 164.310(a) and device and media controls at 45 CFR 164.310(d). Section 164.310(c), the standard for workstation security, also is not accompanied by standalone addressable or required implementation specifications, but it does require a regulated entity to implement physical safeguards that restrict all workstations, such as a laptop or desktop computer or any other device that performs similar functions, that access ePHI to authorized users.[636]

Device and media controls can help regulated entities respond to and recover from security incidents and breaches.[637] Proper understanding of and implementation of such controls may enable regulated entities to quickly determine which devices and electronic media may be implicated in an actual or suspected security incident, or breach, and respond accordingly.[638] For example, if cybercriminals gained access to an organization's network by exploiting a vulnerability present in a particular electronic device, a robust and accurate inventory and tracking process could identify how many devices are affected and where they are located. With this information, a regulated entity should be able to make more effective use of its resources and respond more effectively to an actual or suspected security incident or breach involving such devices. Thus, it is important for regulated entities to implement the device and media controls required under 45 CFR 164.310(d). Accordingly, the standard for device and media controls at 45 CFR 164.310(d), requires a regulated entity to implement policies and procedures to govern how hardware and electronic media containing ePHI are received or removed from a facility and within a facility. Section 164.310(d)(2) includes two required and two addressable implementation specifications. Paragraphs (d)(2)(i) and (ii) on disposal and media re-use, respectively require a regulated entity to implement policies and procedures that address the final disposition of ePHI and the hardware or electronic media on which it is stored, and the removal of ePHI before the electronic media is re-used. Section 164.308(d)(2)(iii) addresses the

[631] ''Considerations for Securing Electronic Media and Devices,'' Office for Civil Rights, U.S. Department of Health and Human Services, p. 1 (Aug. 2018), *https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-august-2018-device-and-media-controls.pdf.*

[632] *See, e.g.,* Sonali Sachdeva, et al., ''Unraveling the role of cloud computing in health care system and biomedical sciences,'' Heliyon (Apr. 2, 2024) (''These days numerous commercial merchants are intermingling with hospitals as well as healthcare providers to establish healthcare-based cloud computing networks.''), *https://www-ncbi-nlm-nih-gov.hhsnih.idm.oclc.org/pmc/articles/PMC11004887/; see also id.* (''[. . .] Microsoft, Google and Amazon have instantly realized that the majority of hospitals will not continue working with servers that are privately owned as well as controlled.''); ''Increase in health-care cyberattacks affecting patients with cancer,'' *supra* note 180 (In 2021, an attack against oncology services targeted data stored in cloud-based systems and affected patients in several States.).

[633] *See* 45 CFR 164.304 (definition of ''Physical safeguards'').

[634] 45 CFR 164.310(a)(2)(i).

[635] 45 CFR 164.310(b).

[636] 45 CFR 164.310(c).

[637] ''Considerations for Securing Electronic Media and Devices,'' *supra* note 631, p. 2.

[638] *Id.*

maintenance of a record of the movement of hardware and electronic media and any person responsible for such hardware or electronic media, while the provision on data backup and storage at 45 CFR 164.310(d)(2)(iv) addresses the creation of a retrievable, exact copy of ePHI before moving the equipment.

2. Issues To Address

The Department has concerns regarding the effectiveness of the language used in the physical safeguards in 45 CFR 164.310 for the same reasons discussed in the context of 45 CFR 164.306 and 164.316. For example, while 45 CFR 164.310 contemplates that a regulated entity must implement the standards and implementation specifications required under 45 CFR 164.310 in accordance with the general documentation and maintenance requirements found in 45 CFR 164.306 and 164.316, at least one court has stated that compliance obligations are limited to the plain words of regulatory text and that a requirement to ''implement'' does not mean that a requirement must be in place throughout the regulated entity's enterprise.[639] Additionally, the standards for facility access controls, workstation use, and device and media controls all require a regulated entity to implement policies and procedures, while the standard for workstation security requires regulated entities to implement physical safeguards. The differences in regulatory text among these provisions could be interpreted to mean that a regulated entity's obligations differ depending on whether a provision requires it to implement only policies and procedures or whether the provision requires the implementation of something more. This may confuse regulated entities and lead some to believe that less comprehensive protection is needed for ePHI subject only to policies and procedures.

The Department believes that the current Security Rule provides a clear path for regulated entities to protect the confidentiality, integrity, and availability of ePHI. However, as discussed above, we also believe recent caselaw has created confusion about the steps regulated entities must take to adequately protect the confidentiality, integrity, and availability of ePHI, as required by the statute. Further, the conditions highlighted by caselaw may also cause regulated entities to misinterpret the regulatory text that connects the current maintenance requirement at 45 CFR 164.306(e), the documentation requirement at 45 CFR 164.316, and the requirement to implement physical safeguards. For example, regulated entities may be confused about how 45 CFR 164.316 requires a regulated entity to document the policies and procedures for specific physical safeguard in 45 CFR 164.310 (or across any other safeguard). In this case, the regulated entity also might not apply the implementation specifications to retain, make available, and review documentation of how it has operationalized the physical safeguard. Failing to connect these provisions would lead to inadequate protection of ePHI and/or an inability to demonstrate compliance with the Security Rule.

Our experience enforcing the Security Rule provides examples of the types of breaches that can occur because of absent or insufficient physical safeguards:

- An investigation of a large health system indicated potential failures to implement policies and procedures and facility access controls to limit physical access to the electronic information systems housed within a large data support center. While the health system did have video surveillance, the investigation found indications that laptops were stored in an interior room that was unlocked and the facility did not have an alarm system.[640]
- A large university hospital experienced a breach of unsecured PHI when it lost an unencrypted flash drive and unencrypted laptop. The Department's investigation found that the covered entity may have failed to use device and media controls, which might have prevented the loss of these devices.[641]

Given the increased portability of devices, media, workstations, and information systems, such components may often be located outside of a regulated entity's physical location. For example, OCR has investigated several incidents involving portable electronic media and mobile workstations that were removed from the regulated entity's physical environment and subsequently lost. As a result, the Department believes that we should more broadly construe the physical environment where ePHI is stored and accessed because it is essential that regulated entities have policies and procedures in place to address the portability of components of their information systems, as well as the ability of workforce members to access such information systems offsite using portable workstations.

Additionally, the standard for device and media controls at 45 CFR 164.310(d)(1) applies only to devices and media, rather than all technology assets that may be components of a regulated entity's relevant electronic information systems. The Department is concerned that a regulated entity may have other types of technology assets that may either create, receive, maintain, or transmit ePHI or otherwise affect its confidentiality, integrity, or availability and that can be removed from, brought to, or moved within its facilities. The confidentiality, integrity, or availability of the regulated entity's ePHI could be negatively affected in the absence of written policies and procedures governing the movement of such technology assets.

Finally, we believe that it is important to address several issues in the standards and implementation specifications for the physical safeguards that are also addressed in other proposals: addressing the Department's expectations regarding implementation specifications;[642] memorializing policies and procedures in writing; documenting the implementation of the aforementioned policies and procedures; reviewing such policies and procedures on a regular cadence; modifying such policies and procedures when reasonable and appropriate;[643] and clarifying the scope of the electronic information systems and their components that regulated entities are expected to consider when establishing their policies and procedures.[644]

3. Proposals

The Department proposes to retain the four standards that comprise the Security Rule's physical safeguards required by 45 CFR 164.306 and codified in 45 CFR 164.310. However, we propose several modifications to 45 CFR 164.310 to address the issues identified above.

a. Section 164.310—Physical Safeguards

The Department proposes to expand the introductory language at 45 CFR

[639] *See University of Texas M.D. Anderson Cancer Center, supra* note 258, p. 479.

[640] Resolution Agreement, ''Advocate Health Care Network Medical Group,'' Office for Civil Rights, U.S. Department of Health and Human Services (July 8, 2016).

[641] Resolution Agreement, ''University of Rochester Medical Center,'' Office for Civil Rights, U.S. Department of Health and Human Services (Oct. 30, 2019) (describing a violation of the standard for device and media controls).

[642] *See* discussion of 45 CFR 164.306.

[643] *See University of Texas M.D. Anderson Cancer Center, supra* note 258.

[644] *See* 45 CFR 164.304 (proposed definitions of ''Relevant electronic information systems'' and ''Technology assets'').

164.310 to clarify that the Security Rule requires that physical safeguards be applied to all ePHI in the possession of the regulated entity, that is, throughout the regulated entity's facilities. The Department also proposes to expand this section to expressly require a regulated entity to implement physical safeguards in accordance with not only 45 CFR 164.306, but also 45 CFR 164.316 to connect the overarching documentation requirements.

Consistent with the proposals to revise the general requirements in 45 CFR 164.306(c) and (d), the Department proposes to remove any distinction between addressable and required implementation specifications in this section such that all specifications would be required. Also consistent with changes proposed elsewhere in this NPRM, the Department proposes to modify all four physical safeguard standards to require that the requisite policies and procedures be in writing[645] and implemented throughout the enterprise.[646] Under this proposal, a regulated entity that could not produce a written policy describing how it will implement a required physical safeguard and demonstrate that the safeguard is in effect and operational throughout the enterprise would not be in compliance with the standard. Consistent with our proposals to require that regulated entities maintain their administrative safeguards, the Department also proposes to require a regulated entity to maintain its security measures by reviewing and testing the required security measures at least once every 12 months, and by modifying the same as reasonable and appropriate. Additionally, we propose to modify certain standards and implementation specifications to ensure that regulated entities understand their obligations to ensure the confidentiality, integrity, and availability of ePHI by implementing physical safeguards to protect their relevant electronic information systems and/or the technology assets in their relevant electronic information systems.

b. Section 164.310(a)(1)—Standard: Facility Access Controls

The Department proposes to modify the standard for facility access controls at 45 CFR 164.310(a)(1) to clarify that the policies and procedures required by this standard must be in writing and address physical access to all of a regulated entity's relevant electronic information systems and the facility or facilities in which these systems are housed and to add a paragraph to clarify the organization of the regulatory text. The Department also proposes to modify the implementation specifications associated with the standard for facility access controls. Specifically, we propose to modify the implementation specifications for contingency operations, facility security plan, and access control and validation procedures at 45 CFR 164.310(a)(2)(i) through (iii) to clarify that we expect a regulated entity to not only establish and implement policies and procedures, but also that we expect them to be in writing.

The Department's proposal would also require that the procedures for contingency operations proposed at 45 CFR 164.310(a)(2)(i) support the regulated entity's contingency plan, instead of the current requirement specifying that the procedures support the restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.[647] This proposal would align the implementation specification for contingency operations with the standard for contingency planning at proposed 45 CFR 164.308(a)(13)(i) by specifically ensuring that the written policies and procedures support the required contingency plan. It also would avoid duplicating the implementation specification for disaster recovery planning at proposed 45 CFR 164.308(a)(13)(ii)(D), which would require a regulated entity to address the restoration of lost data and systems in the disaster recovery plan component of its contingency plan. We propose to modify 45 CFR 164.310(a)(2)(ii) to clarify that the written policies and procedures that constitute the facility security plan must apply to all of the regulated entity's facilities and equipment contained within those facilities. The Department proposes to retitle the implementation specification for access control and validation procedures at 45 CFR 164.310(a)(2)(iii) as ''Access management and validation procedures'' and to require regulated entities to establish and implement written procedures to both authorize and manage a person's role-based access to facilities.

In the implementation specification for maintenance records, the Department proposes at 45 CFR 164.310(a)(2)(iv), to change the provision heading to ''Physical maintenance records'' and to add security cameras to the list of examples of physical security components about which a regulated entity is required to implement written policies and procedures to document repairs and modifications. Both proposals are consistent with and recognize the evolution of the role that technology plays in managing and granting physical access to facilities.

Consistent with our proposals to add maintenance requirements where we believe it is necessary for regulated entities to review, test, and modify their security measures on a particular cadence, we also propose to add an implementation specification for maintenance at proposed 45 CFR 164.310(a)(2)(v). The maintenance provision would require that, for each facility, a regulated entity review and test its written policies and procedures at least once every 12 months, and to modify those policies and procedures as reasonable and appropriate based on that review.

c. Section 164.310(b)(1)—Standard: Workstation Use and Section 164.310(c)—Standard: Workstation Security

Further, in the standards for workstation use and workstation security at 45 CFR 164.310(b) (redesignated as proposed 45 CFR 164.310(b)(1) and (c), respectively), the Department proposes several changes that would recognize the increasingly mobile nature of ePHI and workstations that connect to the information systems of regulated entities. The purpose of these proposals is to ensure that regulated entities properly consider physical safeguards for all workstations, including those that are mobile, and not only those that are located in regulated entities' facilities. The Department also proposes to modify both standards to clarify the organization of the regulatory text. The Department proposes to modify the standard for workstation use to clarify that policies and procedures established by a regulated entity to govern the use of workstations be in writing and address all workstations that access ePHI or the regulated entity's relevant electronic information systems. These proposed changes are consistent with the Department's longstanding expectations and other proposals in this NPRM described above. In 45 CFR 164.310(b)(2)(i)(C), the Department proposes to require a regulated entity to establish and implement written policies and procedures that, among other things, specify the physical attributes of workstation surroundings, including the removal of workstations from a facility and the movement of workstations within and outside of a facility. This proposal is consistent with

[645] *See* discussion of proposals to revise 45 CFR 164.316.

[646] *See* 45 CFR 164.304 (proposed definition of ''Implement'').

[647] *See* proposed 45 CFR 164.308(a)(13).

the proposed revision to the definition of ''workstation'' discussed above. Additionally, we propose to add an implementation specification for maintenance at proposed 45 CFR 164.310(b)(2)(ii) to require that a regulated entity review and test its written policies and procedures at least once every 12 months, and to modify those policies and procedures as reasonable and appropriate based on that review.

Relatedly, the Department proposes to modify the standard for workstation security at 45 CFR 164.310(c) to require a regulated entity to implement physical safeguards for workstations that access ePHI or relevant electronic information systems to comply with its written policies and procedures for workstation use. This proposal would also make clear that such physical safeguards must be modified in response to any modifications to the written policies and procedures for workstation use. As part of their policies and procedures for workstation security, the Department encourages regulated entities to consider, among other things, whether there are workstations located in public areas or other areas that are more vulnerable to theft, unauthorized use, or unauthorized viewing; whether such devices should be relocated; the physical security controls for workstations that are in use (*e.g.,* cable locks, privacy screens, secured rooms, cameras) and whether they are easy to use; and whether there are additional physical security controls that could reasonably be put into place.[648] Additionally, consistent with the Department's proposal to require that a regulated entity provide role-based security awareness training on its Security Rule policies and procedures,[649] the Department expects that such training would address the physical safeguards it has implemented, particularly those policies and procedures for mobile devices that are used to create, receive, maintain, or transmit ePHI or that otherwise affect the confidentiality, integrity, or availability of ePHI.

d. Section 164.310(d)(1)—Standard: Technology Asset Controls

The Department proposes to modify the standard at 45 CFR 164.310(d)(1) by changing the heading to ''Technology asset controls'' from ''Device and media controls,'' and replacing ''hardware and electronic media'' in 45 CFR 164.310(d)(1) and (2) with ''technology assets.'' We believe that this modification would more accurately capture the various categories of components of a regulated entity's relevant electronic information systems that may be received in, removed from, or moved within a facility and that also affect the confidentiality, integrity, or availability of ePHI. Thus, we believe that this modification would provide regulated entities with a clearer understanding of their compliance obligations with respect to the physical safeguards that should be implemented to protect ePHI when technology assets are received by, removed from, or moved within a facility. While we are not proposing other significant changes to 45 CFR 164.310(d)(1) at this time, we remind regulated entities to consider the appropriateness of the policies and procedures they have implemented with respect to the movement of technology assets that maintain ePHI into and out of their facilities and the movement of these items within their facilities. The processes a regulated entity chooses to implement to govern the movement of technology assets may vary based on the type of technology asset.[650] For example, once installed, a server or desktop computer may not need to be moved for the entirety of its lifecycle within the regulated entity, while portable electronic devices and media, such as smartphones, tablets, and USB flash drives are designed to be mobile and may move frequently into, out of, and within a regulated entity's facilities.[651] Thus, the regulated entity's policies and procedures must account for these differences.[652] Further, we note that the proposed definition of workstation includes mobile devices. Mobile devices that serve as workstations are subject to the requirements in this paragraph and those in paragraphs (b) and (c).

The Department also proposes to modify the standard at 45 CFR 164.310(d)(1) to clarify the organization of regulatory text and to clarify its longstanding expectations that policies and procedures must be in writing and to replace ''contain'' with ''maintain,'' consistent with terminology used throughout the HIPAA Rules. The Department believes that having written policies for the disposal of ePHI and the technology assets on which it is stored and for the removal of ePHI from electronic media such that the ePHI cannot be recovered continues to be important to ensuring the physical safety of ePHI. Improper disposal of technology assets puts the ePHI stored in or on such assets at risk for a potential breach, and as discussed elsewhere, data breaches can result in substantial costs to regulated entities and the individuals affected by the breach. We also propose in the related implementation specifications at 45 CFR 164.310(d)(2)(i) and (ii) to require that written policies and procedures for disposal of ePHI and sanitization of electronic media be tied to current standards for sanitizing electronic media before the media are made available for re-use.[653] For example, photocopiers today are often connected to the same network as workstations and generally store the information, including ePHI, transmitted to them. This capability is a significant change from photocopier capabilities that existed when the Security Rule was first issued in 2003. Under this proposal, a regulated entity would be required to include in its written policies and procedures for disposing of ePHI, and the technology assets on which it is maintained, policies and procedures addressing ePHI maintained on photocopiers, consistent with the current standards for disposing and removing ePHI from electronic media.[654]

We have previously explained in guidance that a regulated entity should consider all of the following as part of its risk analysis:

- Disposal of hardware and software, and the documentation of such disposal.
- Destruction of ePHI in such a manner that it cannot be recreated.
- Secure removal of ePHI that was previously stored on hardware or electronic media such that it cannot be accessed and reused.
- The identification of all removable media and their use (*e.g.,* CDs/DVDs, USB flash drives).

[648] *See* ''Workstation Security: Don't Forget About Physical Security,'' Office for Civil Rights, U.S. Department of Health and Human Services, p. 2 (May 2018), *https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-may-2018-workstation-security.pdf.*

[649] *See* proposed 45 CFR 164.308(a)(11)(ii)(A)(*1*).

[650] ''Considerations for Securing Electronic Media and Devices,'' *supra* note 631, p. 1.

[651] *Id.*

[652] *See id.* for a list of questions that regulated entities should consider when developing their policies and procedures regarding device and media controls.

[653] *See* Richard Kissel, et al., ''Guidelines for Media Sanitization,'' NIST Special Publication 800–88, Revision 1, National Institute of Standards and Technology, U.S. Department of Commerce (Dec. 2014), *https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final; see also* ''Proper Disposal of Electronic Devices,'' Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security (Feb. 1, 2021), *https://www.cisa.gov/news-events/news/proper-disposal-electronic-devices.*

[654] *See* ''Guidelines for Media Sanitization,'' *supra* note 653; *see also* ''Proper Disposal of Electronic Devices,'' *supra* note 653.

• The removal of all ePHI from reusable media before the media are reused.[655]

Our guidance describes these considerations in greater detail. For example, regulated entities should consider how to address the replacement of technology assets, including devices and media.[656] Technology assets that need to be replaced should be decommissioned, meaning that they are taken out of service before the final disposition of such assets.[657] Steps a regulated entity should consider as part of its decommissioning process include: ensuring technology assets are securely erased and then either securely destroyed or recycled; ensuring that the regulated entity's technology asset inventory is updated to accurately reflect the status of decommissioned technology assets or technology assets slated to be decommissioned; and ensuring that privacy is protected through proper migration to another electronic information system or total destruction of the ePHI.[658]

The Department proposes to remove the implementation specifications for accountability and data backup and storage at 45 CFR 164.310(d)(2)(iii) and (iv). We believe that the accountability provisions would be subsumed and replaced by the proposed standard for technology asset inventory at proposed 45 CFR 164.308(a)(1)(i). Thus, when the proposed new standard and implementation specifications are read together, the written policies and procedures that govern the receipt and removal of technology assets that maintain ePHI into and out of a facility, and the movement of these assets within the facility, should include tracking relevant information in the technology asset inventory. Similarly, we are proposing to delete the specification for data backup and storage because it is redundant to the administrative safeguard on data backups at proposed 45 CFR 164.308(a)(13)(ii)(B).

As referenced above, in place of the implementation specifications we are proposing to delete, the Department proposes a new implementation specification at proposed 45 CFR 164.310(d)(2)(iii) that would require a regulated entity to review and test the written policies and procedures related to the implementation specifications for technology assets at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate. Such environmental or operational changes may range from new and emerging threats to the confidentiality, integrity, or availability of ePHI (*e.g.,* a new virus) to the adoption of new technology assets by the regulated entity (*e.g.,* a new operating system, new types of workstations). Given the constant evolution of IT and methods for restoring data that has been disposed of or was on electronic media that has been sanitized, the Department believes that it is essential for a regulated entity to at least consider the reasonableness and appropriateness of its policies and procedures for disposal and electronic media sanitation, not only annually, but also in the face of any environmental or operational changes. We expect that pursuant to our proposals to strengthen the standard for risk analysis, a regulated entity would be able to identify such environmental and operational changes before they occur.

4. Request for Comment

The Department requests comment on the foregoing proposals, including any benefits, drawbacks, or unintended consequences. We also request comment on the following considerations in particular:

a. Whether every 12 months is an appropriate frequency for review of a regulated entity's written policies and procedures for physical safeguards. If not, please explain.

b. Whether the written policies and procedures for physical safeguards should be reviewed at different intervals, based on the specific standard or implementation specification. If so, please explain.

c. Whether the Department should include additional examples in regulatory text at proposed 45 CFR 164.310(a)(2)(iv) of physical components of a facility related to security for which there should be written policies and procedures to document repairs and modifications.

d. Whether the standard at proposed 45 CFR 164.310(d)(1) and its associated implementation specifications at paragraph (d)(2) should apply to technology assets that do not maintain ePHI, but do access the regulated entity's relevant electronic information systems.

F. Section 164.312—Technical Safeguards

1. Current Provisions

Section 164.312 includes five standards for technical safeguards, which are the requirements concerning the implementation of technology and technical policies and procedures to protect the confidentiality, integrity, and availability of ePHI and related information systems. A regulated entity must comply with the standards for technical safeguards in accordance with 45 CFR 164.306(c), the provision that describes the general rules for the security standards.

Under 45 CFR 164.312(a)(1), a regulated entity is required to establish policies and procedures for electronic information systems to allow access only to those persons or software programs that have been granted access rights as specified in 45 CFR 164.308(a)(4). Regulated entities may comply with this standard by implementing a combination of access control methods and technical controls, consistent with the implementation specifications for this standard. The Security Rule does not identify a specific access control method or technology to implement. Regardless of the technology or information system used, access controls should be appropriate for the workforce member's role and/or function.[659] For example, a workforce member responsible for monitoring and administering information systems with ePHI, such as an administrator or a superuser,[660] should only have access to ePHI as appropriate for their role and/or job function.

The implementation specifications that provide instructions for satisfying the access control standard are found at 45 CFR 164.312(a)(2). Two are required and two are addressable.[661] The implementation specifications address unique user identifiers,[662] emergency access procedures,[663] automatic logoff,[664] and encryption and decryption.[665] The implementation

[655] ''Guidance on Disposing of Electronic Devices and Media,'' Office for Civil Rights, U.S. Department of Health and Human Services, p. 1 (July 2018), *https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-july-2018-Disposal.pdf.*

[656] *Id.* at 2.

[657] *Id.*

[658] *Id.*

[659] ''Security Standards: Technical Safeguards,'' *supra* note 343, p. 4.

[660] A superuser is ''a user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.'' NIST definition of ''superuser,'' Glossary, Computer Security Resource Center, National Institute of Standards and Technology, U.S. Department of Commerce, *https://csrc.nist.gov/glossary/term/superuser.*

[661] *See* 45 CFR 164.306(d) for an explanation of ''required'' and ''addressable'' implementation specifications.

[662] 45 CFR 164.312(a)(2)(i).

[663] 45 CFR 164.312(a)(2)(ii).

[664] 45 CFR 164.312(a)(2)(iii).

[665] 45 CFR 164.312(a)(2)(iv).

specification for unique user identification requires a regulated entity to assign unique identifiers to users to facilitate the identification of specific users of an information system.[666] By assigning a unique identifier to each user, a regulated entity can track the specific activity of that user when they are logged into an information system and hold the user accountable for functions they perform in the information system when they access that system.

Under the implementation specification for emergency access procedures, a regulated entity is required to establish procedures, such as documented operational practices and instructions to workforce members, for obtaining access to necessary ePHI during an emergency and to implement such procedures as needed.[667] In accordance with this implementation specification, a regulated entity must identify the types of situations in which its normal procedures for accessing an information system or application that contains ePHI may not work and establish procedures for obtaining access in those situations.[668] These procedures must be established prior to an emergency to instruct workforce members on possible ways to gain access to needed ePHI where, for example, the electrical system has been severely damaged or rendered inoperative, or where a software update fails and prevents the regulated entity from accessing ePHI in its EHR.

The implementation specification for automatic logoff associated with the standard for access control addresses the need for a regulated entity to, when reasonable and appropriate, implement electronic procedures that terminate an electronic session after a period of inactivity.[669] Automatic logoff is an effective way to prevent unauthorized users from accessing ePHI on a workstation when it is left unattended for a period of time.[670] While many applications have configuration settings that automatically log a user out of the system after a period of inactivity, some systems have more limited capabilities and may activate a screen saver that is password protected.[671]

The implementation specification under the standard for access control addresses encryption and decryption and requires regulated entities, when it is reasonable and appropriate, to implement a mechanism to encrypt and decrypt ePHI.[672] Encrypting data, including ePHI, reduces the likelihood that anyone other than the party that has the key to the encryption algorithm would be able to decrypt (*i.e.,* translate) the data and convert it into plain, comprehensible text.[673]

The standard for audit controls requires a regulated entity to implement hardware, software, and/or procedural mechanisms that record and examine activity in electronic information systems that contain or use ePHI. Most electronic information systems provide some level of audit controls with a reporting method, such as audit reports.[674] These controls are useful for recording and examining information system activity, especially when determining whether a security violation has occurred.[675] The Security Rule does not identify data that must be gathered by the audit controls or how often the audit reports should be reviewed.[676] Instead, a regulated entity must consider its risk analysis and organizational factors, such as current technical infrastructure and hardware and software security capabilities, to determine reasonable and appropriate audit controls for information systems that contain or use ePHI.[677] The audit controls standard has no implementation specifications.

Section 164.312(c)(1), the standard for integrity, requires a regulated entity to implement policies and procedures to protect ePHI from improper alteration or destruction. The integrity of data can be compromised by both technical and non-technical sources. Workforce members or business associates may make accidental or intentional changes that improperly alter or destroy ePHI. Data can also be altered or destroyed without human intervention, such as by electronic media errors or failures.[678] The purpose of this standard is to establish and implement policies and procedures for protecting ePHI from being compromised regardless of the source. Improperly altered or destroyed ePHI can result in clinical quality problems for a covered entity, including patient safety issues.[679]

Section 164.312(c)(2) contains the addressable implementation specification for the integrity standard that requires a regulated entity, when reasonable and appropriate, to implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner. To determine which electronic mechanisms should be implemented to ensure the integrity of ePHI, a regulated entity must consider the various risks to the integrity of ePHI identified during the risk analysis. Once a regulated entity has identified risks to the integrity of its data, it must identify security measures that will reduce the risks.[680]

The standard for person or entity authentication at 45 CFR 164.312(d) requires a regulated entity to establish policies and procedures for verifying that a person seeking access to ePHI is the one claimed. This standard addresses technical controls for ensuring access is allowed only to those persons or software programs that have been granted access rights under the administrative safeguard for information access management at 45 CFR 164.308(a)(4). This standard has no implementation specifications.

Under the standard for transmission security at 45 CFR 164.312(e)(1), a regulated entity is required to implement technical security measures to guard against unauthorized access to ePHI when transmitted electronically, such as through the internet. A regulated entity must identify the available and appropriate means to protect ePHI as it is transmitted, select appropriate solutions, and document its decisions.[681]

The two addressable implementation specifications for the transmission security standards are under 45 CFR 164.312(e)(2). The implementation specification for integrity controls requires a regulated entity, when it is reasonable and appropriate, to implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until the ePHI has been disposed.[682] The implementation specification for encryption requires a regulated entity, when it is reasonable and appropriate, to implement a mechanism to encrypt ePHI.

[666] 45 CFR 164.312(a)(2)(i).

[667] 45 CFR 164.312(a)(2)(ii).

[668] ''Security Standards: Technical Safeguards,'' *supra* note 343, p. 5.

[669] 45 CFR 164.312(a)(2)(iii).

[670] ''Security Standards: Technical Safeguards,'' *supra* note 343, p. 6.

[671] *Id.*

[672] 45 CFR 164.312(a)(2)(iv).

[673] ''Security Standards: Technical Safeguards,'' *supra* note 343, p. 7.

[674] ''Understanding the Importance of Audit Controls,'' Cybersecurity Newsletter, Office for Civil Rights, U.S. Department of Health and Human Services, p. 1 (Jan. 2017), *https://www.hhs.gov/sites/default/files/january-2017-cyber-newsletter.pdf?language=es.*

[675] *Id.*

[676] *Id.* at 2.

[677] *Id.*

[678] ''Security Standards: Technical Safeguards,'' *supra* note 343, p. 7.

[679] *Id.*

[680] *Id.* at 9.

[681] *Id.* at 10.

[682] 45 CFR 164.312(e)(2)(i).

2. Issues To Address

While the intention of 45 CFR 164.312 is for regulated entities to develop and put into place technical controls, the Department is aware that regulated entities have not always achieved the degree of protection for ePHI that we intended. Absent a definition of ''implement,'' some regulated entities might interpret the term to mean something other than implementing technical controls to ensure the confidentiality, integrity, and availability of ePHI. This misinterpretation may leave ePHI partially unprotected because regulated entities may not implement safeguards throughout their enterprise. As discussed above with respect to both the administrative and physical safeguards, the Department is also concerned that regulated entities are not making the connection between the maintenance requirement at 45 CFR 164.306(d) and the requirement to implement technical safeguards, and therefore, are not reviewing or updating their policies and procedures for technical safeguards. Additionally, the Department believes that regulated entities may not be recognizing that their obligations under the Security Rule to protect ePHI are not limited to protecting electronic information systems that create, receive, maintain, or transmit ePHI, but necessarily include other electronic information systems that affect the confidentiality, integrity, or availability of ePHI.

While the Security Rule relies on a flexible and scalable approach to compliance, the health care industry's shift to a digital environment has substantially increased both the risk to ePHI and the prevalence of technological solutions for addressing those risks. Additionally, the cost of such solutions has, in many cases, decreased over time, as is often the case with technology. For example, when the original Security Rule was published, tools to encrypt ePHI had limited availability, were more costly, and were not user-friendly, particularly for small health care providers.[683] By contrast, in 2024, the technical ability to encrypt data may be seamless in many applications, inexpensive, and widely available in commercial software and hardware products.[684] Where an encryption solution is not integrated into an application, software, or hardware, third-party solutions are often available.[685] Thus, we do not believe that it is appropriate for such provisions to be ''addressable.'' [686]

Based on its own investigations and compliance reviews, news reports, and published studies, the Department is aware that many regulated entities have failed to implement adequate technical controls, or, in some cases, any technical controls. For example:

- A large health system that operates in multiple States experienced a massive data breach resulting from a hacking incident. OCR's investigation found indications of potential failures to sufficiently monitor its activity in its information systems that was insufficient to protect against a cyberattack, implement an authentication process to safeguard its ePHI, and have security measures in place to protect ePHI from unauthorized access when it was being transmitted electronically.[687]
- A Rhode Island nonprofit health system experienced a data breach resulting from the theft of a laptop. OCR's investigation found indications of potential failures to encrypt ePHI, despite the entity's determination to implement encryption, and a lack of device and media controls.[688]
- At a large covered entity, workforce members used their log-in credentials to access medical records maintained in the entity's EHR without a job-related purpose.[689] OCR's investigation found evidence of potential violations of the requirement to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule.[690]
- At another covered entity, the potential failure to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI, among other things, enabled a workforce member to sell the ePHI of more than 12,000 individuals.[691]

Some investigations have found indications that regulated entities may implement technical controls that address some, but not all, users of and technology assets in a relevant electronic information system, such as software, hardware, and persons involved in the development, configuration, and implementation of technical controls.[692] And other investigations have suggested that the potential failure of a regulated entity to have security measures in place to protect ePHI from unauthorized access when it is transmitted electronically has resulted in increased risk and breaches of ePHI.[693] Common network segmentation practices would have substantially reduced the risk to the security ePHI and could have prevented such breaches.

Beyond the health care sector, threat actors have been able to gain access to networks by compromising user accounts and taking advantage of insufficient network segregation. For example, the 2014 Home Depot breach involved the compromise of a third-party vendor's username and password to enter Home Depot's network, which allowed hackers to obtain elevated rights to navigate to self-checkout point-of-sale system.[694] The Department is concerned about the potential effects of such incidents in health care, where they would jeopardize the confidentiality, integrity, and availability of ePHI.

Finally, consistent with the concerns expressed above about the implications of recent caselaw and the uncertainty it might cause among regulated entities assessing whether they have adequately protected their ePHI, the Department is concerned that the existing Security Rule may not provide sufficient instruction to regulated entities about

---

[683] 68 FR 8334, 8357 (Feb. 20, 2003).

[684] For example, the ONC Health IT Certification Program requires that certified health IT certified to the end-user device encryption certification criterion at 45 CFR 170.315(d)(7) must encrypt electronic health information stored on end-user devices after use of the technology on those devices stops or prevent electronic health information from being locally stored on end-user devices after use of the technology on those devices stops. *See also* ''Security Standards: Technical Safeguards,'' *supra* note 343, p. 7.

[685] ''How to Protect the Data that is Stored on Your Devices,'' Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security (access July 26, 2024), *https://www.cisa.gov/resources-tools/training/how-protect-data-stored-your-devices; see also* Karen Scarfone, et al., ''[Information Technology Laboratory (ITL)] Bulletin: August 2020, Security Considerations for Exchanging Files Over the internet,'' National Institute of Standards and Technology, U.S. Department of Commerce (Aug. 2020), *https://csrc.nist.gov/files/pubs/shared/itlb/itlbul2020-08.pdf.*

[686] 45 CFR 164.306(d).

[687] ''Banner Health,'' *supra* note 567.

[688] Resolution Agreement, ''Lifespan,'' Office for Civil Rights, U.S. Department of Health and Human Services (June 26, 2020), *https://www.hhs.gov/sites/default/files/lifespan-ra-cap-signed.pdf.*

[689] Resolution Agreement, ''Yakima Valley Memorial Hospital,'' Office for Civil Rights, U.S. Department of Health and Human Services (May 15, 2023), *https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/yakima-ra-cap/index.html.*

[690] *Id.*

[691] *See* ''Montefiore Medical Center,'' *supra* note 248.

[692] *See, e.g.,* ''HHS Office for Civil Rights Settles HIPAA Investigation with Arizona Hospital System Following Cybersecurity Hacking,'' *supra* note 570.

[693] *Id.*

[694] ''The Home Depot Reports Findings in Payment Data Breach Investigation,'' Home Depot (Nov. 6, 2014), *https://ir.homedepot.com/news-releases/2014/11-06-2014-014517315.*

how they must maintain specific security measures.

3. Proposals

The Department retains the requirements for technical safeguards generally and proposes additions and modifications to the existing standards and implementation specifications.

a. Section 164.312—Technical Safeguards

The Department proposes to expand the primary provision at 45 CFR 164.312 to clarify that regulated entities as a general matter must implement and document the implementation of technical safeguards adopted for compliance with the Security Rule. This proposal would clarify that the requirement to implement and document technical safeguards would apply to all technical safeguards, including technical controls, implemented by a regulated entity to protect the confidentiality, integrity, and availability of all ePHI it creates, receives, maintains, or transmits.

As noted above, the current provision at 45 CFR 164.312 does not reference the documentation requirements in 45 CFR 164.316. Therefore, for clarity, we propose to explicitly require in 45 CFR 164.312 that documentation of technical safeguards conforms to the requirements in 45 CFR 164.316. This proposed change would clarify that a regulated entity must document the policies and procedures required to comply with this rule and how entities considered the flexibility factors in 45 CFR 164.306(b). It would also clarify that a regulated entity must document each action, activity, and assessment required by the Security Rule. The Department considers the documentation requirements and other provisions of 45 CFR 164.316 to apply to all of the safeguards, including the technical safeguards, and this proposal is intended to remove any potential uncertainty among regulated entities. Additionally, we propose to add maintenance requirements separately to the implementation specifications for particular technical safeguards in 45 CFR 164.312, as discussed below and consistent with our proposals to add similar requirements to particular administrative and physical safeguards.

Additionally, as discussed above, the Department proposes to remove the distinction between required and addressable implementation specifications and make all implementation specifications required, with specific, limited exceptions. Also as discussed above, we propose to modify certain standards and implementation specifications to clarify that the technical safeguards apply to ensure the confidentiality, integrity, and availability of ePHI, which requires a regulated entity to implement the technical safeguards in or on all relevant electronic information systems. These proposals are discussed in greater detail below.

b. Section 164.312(a)(1)—Standard: Access Control

The Department proposes to clarify the standard for access control at 45 CFR 164.312(a)(1) by requiring a regulated entity to deploy technical controls in relevant electronic information systems to allow access only to those users and technology assets that have been granted access rights. This proposed modification would ensure that a regulated entity deploys technical controls, rather than solely ensuring that it implements technical policies and procedures, consistent with our proposals to define ''deploy'' and ''implement.'' [695] Thus, the proposal would clarify that a regulated entity is not expected to merely establish a policy and procedure, but must also put into place, ensure the operation of, and verify the continued operation of, technical controls for access to its relevant electronic information systems such that the failure to have such technical control in operation throughout its enterprise would be a violation of the new proposed standard. Additionally, the Department's proposal would clarify that access controls would apply to persons with authorized access and to technology assets.

Access controls are one of the key mechanisms by which a regulated entity protects ePHI. Such technical controls ensure that access to the regulated entity's electronic information systems is limited to only users and technology assets that have been granted access rights under the policies and procedures adopted in accordance with the standard for information access management under 45 CFR 164.308.[696] The Security Rule does not identify a specific type of access control method or technology to deploy, nor are we proposing to do so in this rule.[697] As discussed above, access rights should be role-based and the technical controls should assist the regulated entity in implementing such policies and procedures. For example, workforce members responsible for monitoring and administering a regulated entity's relevant electronic information systems, such as someone responsible for cybersecurity or providing technical support to users, must only have access to ePHI and to the regulated entity's relevant electronic information systems as appropriate for their role and job function.

We also propose at 45 CFR 164.312(a)(1) to add a paragraph heading to clarify the organization of the regulatory text.

The Department proposes to modify the existing implementation specifications under the standard for access control and to add five new implementation specifications. Additionally, we propose to redesignate the implementation specification for encryption and decryption as a standard.

We propose to modify the implementation specification for unique user identification at 45 CFR 164.312(a)(2)(i) by renaming the implementation specification as ''Unique identification'' and adding a requirement to assign a unique identifier for tracking each technology asset. These proposed modifications would clarify for regulated entities that the purpose of this requirement is to enable a regulated entity to identify and track unauthorized activity in its relevant electronic information systems. Such unauthorized activity may include activity by unauthorized persons or technology assets. It may also include activity by persons who are authorized to access the regulated entity's relevant information systems but who access ePHI that they do not need to access for their job or function.

The Department also proposes to expand the types of identifiers a regulated entity may assign to users and technology assets beyond names to include numbers and/or other identifiers and to clarify that a unique identifier must be assigned to each user and technology asset in the regulated entity's relevant electronic information systems. This proposed modification would better meet the goals of this implementation specification by requiring a regulated entity to be able to discern and track activities among all users and technology assets, regardless of whether that user or technology asset is a person, hardware, software program, or device. The proposed implementation specification for unique identification aligns with the Department's essential CPG for Unique Credentials, which calls for regulated entities to use unique credentials to

[695] *See* 45 CFR 164.304 (proposed definitions of ''Deploy'' and ''Implement'').

[696] ''Security Standards: Technical Safeguards,'' *supra* note 343, p. 3.

[697] *Id.* at 4.

help detect and track anomalous activities.[698]

Additionally, we propose to add an implementation specification at proposed 45 CFR 164.312(a)(2)(ii) for administrative and increased access privileges. Access controls should enable an authorized user to access the minimum necessary information needed to perform their job functions.[699] Rights and/or privileges should be granted to authorized users based on the policies and procedures required under the administrative safeguard for information access management.[700] For example, a workforce member who has certain role-based administrative access privileges should have separate user identities for non-administrative access privileges and administrative access privileges. Separating a single workforce member's user identities based on access privilege substantially limits the risk that an intruder will be able to access ePHI through a workforce member's user identity when they are using the administrative access privileges.[701] A regulated entity may be able to improve the control and review of the use of administrative access privileges, such as through a privileged access management system, to understand how privileged accounts are used within its environment and help detect and prevent the misuse of privileged accounts.[702]

The proposed implementation specification would require a regulated entity to separate the unique user identities required by the implementation specification for unique user identification based on the type of access privileges used by a specific unique user. For example, the adoption of health IT that is certified through the ONC Health IT Certification Program as having the technical capability to establish user permissions for accessing, and performing actions with, electronic health information based on unique identifiers may contribute to a regulated entity's compliance with the proposed new implementation specification for administrative and increased access privileges, should the proposal be finalized.[703] This proposed new implementation specification aligns with the Department's essential CPG for Separate User and Privileged Accounts by addressing the separation of privileged or administrator access rights from common user accounts.[704]

Additionally, the Department proposes to redesignate the implementation specification for emergency access procedures at 45 CFR 164.312(a)(2)(ii) as proposed 45 CFR 164.312(a)(2)(iii) and to modify it to require a regulated entity to establish both written procedures and technical procedures for obtaining necessary ePHI during an emergency and to implement them as needed. For example, we note that the adoption of health IT that is certified through the ONC Health IT Certification Program as having the technical capability to permit an identified set of users to access electronic health information during an emergency may contribute to a regulated entity's compliance with the proposed implementation specification for emergency access procedures, should the proposal be finalized.[705]

Under the Department's proposal, the implementation specification for automatic logoff at 45 CFR 164.312(a)(2)(iii) would be redesignated as proposed 45 CFR 164.312(a)(2)(iv) and modified to require a regulated entity to deploy technical controls that terminate an electronic session after a period of inactivity. Deploying a mechanism to automatically terminate an electronic session after a period of inactivity reduces the risk of unauthorized access when a user forgets or is unable to terminate their session.[706] Failure to deploy automatic logoff not only increases the risk of unauthorized access and potential alteration or destruction of ePHI; it also impedes an organization's ability to properly investigate such unauthorized access because it would appear to originate from an authorized user.[707]

The Department proposes that the period of inactivity be both predetermined and reasonable and appropriate. When determining the length of the period of inactivity, a regulated entity should consider the access privileges of a given user or technology asset, the system(s) being accessed, the environment in which the system access occurs, and other appropriate factors in determining a reasonable and appropriate time of inactivity before session termination. For example, in an emergency setting, a user may not have time to manually log out of a system. User identities with administrative and other high-level access that present a greater risk to the confidentiality, integrity, and availability of ePHI should have appropriately shorter periods of inactivity because of the increased risk. While many applications have configuration settings for automatic logoff,[708] a regulated entity must determine whether the default automatic logoff is reasonable and appropriate and make modifications if it is not. For example, the adoption of health IT that is certified through the ONC Health IT Certification Program as having the technical capability to automatically stop a user's access to health information after inactivity for a predetermined period and require a user to re-enter their credentials to resume or regain access may contribute to a regulated entity's compliance with the proposed implementation specification for automatic logoff, should the proposal be finalized.[709]

Additionally, we propose to add an implementation specification for log-in attempts at proposed 45 CFR 164.312(a)(2)(v). The proposal would require a regulated entity to deploy technical controls that disable or suspend the access of a user or technology asset to relevant electronic information systems after a certain number of unsuccessful authentication attempts. Although incorrectly keying in a known password by the intended user may occur infrequently, a repeated and persistent failure is a strong indication of an attempt at unauthorized access. For example, brute force attacks are attempts to gain unauthorized access by guessing the password many times in a row.[710] Technical controls that limit the number of incorrect log-in attempts by disabling or suspending the access of a user or technology asset to relevant electronic information systems are appropriate to address unsuccessful login attempts.[711]

The proposal would require a regulated entity to determine the number of unsuccessful authentication attempts that would trigger disabling or suspending access to relevant electronic information system. The number should

[698] ''Cybersecurity Performance Goals,'' *supra* note 18.

[699] *Id.* at 3–4.

[700] *See* 45 CFR 164.308(a)(4) and proposed 45 CFR 164.308(a)(10).

[701] *See* ''Controlling Access to ePHI: For Whose Eyes Only?,'' *supra* note 416.

[702] ''Defending Against Common Cyber-Attacks,'' *supra* note 396.

[703] *See* 45 CFR 170.315(d)(1).

[704] ''Cybersecurity Performance Goals,'' *supra* note 18.

[705] *See* 45 CFR 170.315(d)(6).

[706] ''Controlling Access to ePHI: For Whose Eyes Only?,'' *supra* note 416.

[707] *Id.*

[708] For example, Windows 10 operating system allows users to customize security options to automatically logout a user after a specified period of inactivity.

[709] *See* 45 CFR 170.315(d)(5).

[710] ''Brute Force Attacks Conducted by Cyber Actors,'' Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security (May. 6, 2020), *https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors.*

[711] ''Security and Privacy Controls for Information Systems and Organizations,'' *supra* note 600, p. 39.

be reasonable and appropriate for the type of user or technology asset, the electronic information system or technology asset to which access is sought, and the type of information maintained on such information system or technology asset. For example, a regulated entity may determine that any authentication failure of an administrative privileged access account should disable the account because of the level of risk compared to an authentication failure of a non-administrative privileged account. The Department does not propose to define disable or suspend and relies upon the industry understanding that disabling a user's access would require intervention to restore the capability to use the user identity, while a suspension may prevent additional log-in attempts for a temporary, limited period of time.

Consistent with NCVHS' recommendation and existing guidance, the Department also proposes to add an implementation specification for network segmentation at 45 CFR 164.312(a)(2)(vi) that would require a regulated entity to deploy technical controls to segment its relevant electronic information systems in a reasonable and appropriate manner.[712] Under this proposal, a regulated entity with multiple, distinct electronic information systems would be required to separate relevant electronic information systems using reasonable and appropriate technical controls. Network segmentation is a physical or virtual division of a network into multiple segments, creating boundaries between the operational and IT networks to reduce risks, such as threats caused by phishing attacks.[713] For example, where a regulated entity operates both a point-of-sale system and an EHR on the same network, the EHR could be compromised through a successful attack by an intruder moving laterally (*i.e.,* within the same network) from a previously compromised point-of-sale system because the intruder's movements were not impeded by network segmentation. Accordingly, we believe that it is appropriate to require regulated entities to deploy technical controls to segment the networks to which their relevant electronic information systems are connected.[714] What constitutes reasonable and appropriate network segmentation depends on the regulated entity's risk analysis and how it has implemented its network(s) and relevant electronic information systems. This proposed new implementation specification aligns with the Department's enhanced CPG for Network Segmentation because where the CPG is implemented, an intruder's ability to freely move within a regulated entity's network and protect ePHI is minimized.[715]

The proposed implementation specification for data controls at proposed 45 CFR 164.312(a)(2)(vii) would require a regulated entity to deploy technical controls to allow access to ePHI based on the regulated entity's policies and procedures for granting users and technology assets access relevant electronic information systems as specified in proposed 45 CFR 164.308(a)(10). This implementation specification would require a regulated entity to have in place technical controls that distinguish between users and technology assets, that are permitted to access the regulated entity's relevant electronic information systems and those that are not permitted to do so and would require that the controls permit or disallow access accordingly.

Properly deployed network-based solutions can limit the ability of a hacker to gain access to an organization's network or impede the ability of a hacker already in the network from accessing other electronic information systems—especially systems containing sensitive data.[716] Access controls could include role-based access, user-based access, or any other access control mechanisms the organization deems appropriate.[717] Access controls need not be limited to computer systems—firewalls, network segmentation, and network access control solutions are effective means of limiting access to relevant electronic information systems.[718]

Additionally, we propose to add an implementation specification for maintenance at proposed 45 CFR 164.312(a)(2)(viii). Under this proposal, a regulated entity would be expressly required to review and test the effectiveness of the procedures and technical controls required by the implementation specifications associated with the standard for access control at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

c. Section 164.312(b)(1)—Standard: Encryption and Decryption

Encryption can reduce the risks and costs of unauthorized access to ePHI.[719] For example, if a hacker gains access to unsecured ePHI on a network server or if a device containing unsecured ePHI is stolen, a breach of PHI will be presumed and reportable under the Breach Notification Rule.[720] The Breach Notification Rule applies to unsecured PHI, which is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance issued under the HITECH Act.[721] The Department's guidance on rendering unsecured PHI unusable, unreadable, or indecipherable to persons who are not authorized to access such PHI states that ePHI at rest (*i.e.,* stored in an information system or electronic media) is considered secured if it is encrypted in a manner consistent with NIST Special Publication 800–111 [722] (''SP 800–111''). The ePHI encrypted in a manner consistent with SP 800–111 is not considered unsecured PHI and therefore qualifies for what is commonly known as the Breach Notification safe harbor, meaning that it is not subject to the requirements of the Breach Notification Rule.[723] Thus, by encrypting ePHI in a manner consistent with the Secretary's guidance, a regulated entity may not only fulfill its encryption obligation under the Security Rule, but also make use of the

[712] *See* Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 3 (recommending that the Department require network segmentation as part of a layered security approach, segregating network components based on user characteristics, such as corporate network compared to business associate network); ''Layering Network Security Through Segmentation,'' Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security, *https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf;* ''Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients,'' *supra* note 16, pp. 23 and 31; PR.IR–01, ''The NIST Cybersecurity Framework (CSF) 2.0,'' *supra* note 15.

[713] ''Layering Network Security Through Segmentation,'' *supra* note 712.

[714] Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 3.

[715] ''Cybersecurity Performance Goals,'' *supra* note 18.

[716] ''Controlling Access to ePHI: For Whose Eyes Only?,'' *supra* note 416.

[717] *Id.*

[718] *Id.*

[719] *Id.*

[720] *See* 45 CFR 402. The presumption applies unless it can be rebutted in accordance with the breach risk assessment described in 45 CFR 164.402(2).

[721] 45 CFR 164.402.

[722] Karen Scarfone, et al., ''Guide to Storage Encryption Technologies for End User Devices: Recommendations of the National Institute of Standards and Technology,'' NIST Special Publication 800–111, National Institute of Standards and Technology, U.S. Department of Commerce (Nov. 2007), *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf.*

[723] 74 FR 19600, 19009–19010 (Apr. 27, 2009).

Breach Notification Rule's safe-harbor provision.[724]

As the use of mobile computing devices (*e.g.,* laptops, smartphones, tablets) has become more pervasive, the risks to sensitive data stored on such devices also have increased.[725] And while in 2003 and even in 2013, encryption might have been out of reach for many regulated entities because of cost or a similar reason,[726] today, encryption solutions are generally considered to be widely accessible. The cost of such solutions has decreased significantly, as has the difficulty in implementing such solutions. In fact, many applications have encryption solutions embedded in them.[727] Once enabled, a device's encryption solution can protect stored sensitive data, including ePHI, from unauthorized access in the event the device is lost or stolen. The same is true for most software today.[728] Thus, while encryption of a particular regulated entity's ePHI might not have been reasonable and appropriate in 2003 or 2013, the Department believes encryption generally is reasonable and appropriate today.[729]

Because the prevalence of encryption solutions has increased, as has their affordability and the role they play in protecting information, including ePHI, the Department believes it is appropriate to consider requiring encryption and elevating it from an implementation specification to a standard to increase its visibility and prominence. Based on this and consistent with NCVHS' recommendation, the Department proposes to redesignate the implementation specification for encryption and decryption at 45 CFR 164.312(a)(2)(iv) as a standard at proposed 45 CFR 164.312(b)(1).[730] The proposed standard would incorporate the requirements of two implementation specifications that address encryption—the one addressed here and the one at 45 CFR 164.312(e)(2)(ii).[731] The Department proposes that the new standard would require a regulated entity to configure and implement technical controls to encrypt and decrypt all ePHI in a manner that is consistent with prevailing cryptographic standards. This proposed new standard aligns with the Department's essential CPG for Strong Encryption by calling for regulated entities to deploy encryption to protect ePHI and with the recommendation of NCVHS.[732] We also note that the adoption of health IT that is certified through the ONC Health IT Certification Program as having the technical capability to encrypt and decrypt electronic health information, using an encryption algorithm that meets certain requirements, may contribute to a regulated entity's compliance with the proposed standard for encryption and decryption, should the proposal be finalized.[733]

Under the proposal, a regulated entity would need to ensure that an encryption solution that it adopts meets prevailing cryptographic standards prior to using it. The Department uses the phrase ''prevailing cryptographic standards'' to refer to widely accepted standards for encryption and decryption that are recommended by authoritative sources and that ensure the confidentiality, integrity, and availability of ePHI at the time the regulated entity performs its risk analysis and establishes or modifies its risk management plan. The Department would expect a regulated entity to deploy updated encryption solutions as prevailing cryptographic standards evolve, consistent with both of the proposed requirements discussed above: (1) to review, verify, and update its risk analysis in response to changes in its environment that may affect ePHI; and (2) to review and modify, as reasonable and appropriate, its risk management plan in response to changes in its risk analysis. Thus, a regulated entity using an encryption algorithm that is known to be insecure would not be in compliance with the proposed requirement to deploy an encryption algorithm that meets prevailing cryptographic standards. We are not proposing to define prevailing cryptographic standards in regulatory text at this time.

The Department proposes to add one implementation specification for the proposed standard for encryption and decryption. Specifically, proposed 45 CFR 164.312(b)(2) would require regulated entities to encrypt all ePHI at rest and in transit, with limited exceptions.[734] Thus, a regulated entity would be required to encrypt all ePHI it maintains, as well as all ePHI it transmits, unless an exception applies, and the following conditions are met:

- Each exception applies only to the ePHI directly affected by the circumstances described in the specific exception.
- Each exception applies only to the extent that the regulated entity documents its understanding that the exception applies to the scenario in which the regulated entity relies upon the exception and why or how the exception applies, and that any additional applicable conditions are met.

The first proposed exception at proposed 45 CFR 164.312(b)(3)(i) would apply to a technology asset currently used by a regulated entity that does not support encryption according to prevailing cryptographic standards. Because the requirements for encryption under the Security Rule today are addressable, a regulated entity may be in compliance with the encryption requirement without actual encryption of ePHI if encryption is not reasonable and appropriate, provided that the entity meets certain conditions. Additionally, technology assets in use today may rely on cryptographic standards that are no longer accepted industry practice. The Department recognizes that it may take some time for a regulated entity to adopt compliant technology assets. Thus, we propose this exception for such technology assets that do not support encryption consistent with prevailing cryptographic standards in limited circumstances. Specifically, to meet this exception, a regulated entity would be required to establish a written plan to migrate ePHI to technology assets that support encryption consistent with prevailing cryptographic standards and to implement such plan. The regulated entity would be required to establish and implement the written plan within

[724] 45 CFR 164.402.

[725] ''Controlling Access to ePHI: For Whose Eyes Only?,'' *supra* note 416.

[726] *See* 68 FR 8334, 8357 (Feb. 20, 2003).

[727] ''Controlling Access to ePHI: For Whose Eyes Only?,'' *supra* note 416.

[728] *Id.*

[729] *See* discussion of 45 CFR 164.312, *infra.*

[730] Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 2.

[731] The Department is also proposing to delete the implementation specification for encryption at 45 CFR 164.312(e)(2)(ii) because we are proposing to address the substantive requirements of that implementation specification in proposed 45 CFR 164.312(b)(2).

[732] ''Cybersecurity Performance Goals,'' *supra* note 18; Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 2.

[733] *See* 45 CFR 170.315(d)(7) and 170.210(a).

[734] For example, adoption of health IT that is certified through the ONC Health IT Certification Program as having the technical capability to encrypt, or prevent the local storage of, electronic health information stored on end-user devices after use of the technology on those devices stops may contribute to a regulated entity's compliance with the proposed implementation specification for encryption and decryption. *See* 45 CFR 170.315(d)(7). Additionally, the proposed implementation specification generally is consistent with the Health Data, Technology, and Interoperability: Patient Engagement, Information Sharing, and Public Health Interoperability (HTI–2) NPRM proposal to modify 45 CFR 170.315(d)(7), should it be finalized, to include requirements that authentication credentials be protected using industry-standard encryption and decryption. *See* 89 FR 63536–37, 63778 (Aug. 5, 2024).

a reasonable and appropriate period of time. For example, it would not be reasonable or appropriate for a regulated entity to establish a plan to migrate ePHI on a single flash drive within 30 days and not complete migration of that ePHI for a period of a year because migrating ePHI from a flash drive to a more secure medium is a simple and quick process that the regulated entity already determined could be completed within 30 days. Thus, a year would be an unreasonably long period to leave ePHI insufficiently encrypted, particularly after a need to migrate the ePHI has been established. In such circumstances, the regulated entity would not be complying with the requirements of this proposed exception.

The second proposed exception at proposed 45 CFR 164.312(b)(3)(ii) would be available for ePHI transmitted in response to an individual request, pursuant to 45 CFR 164.524, to receive their ePHI in an unencrypted manner. Unencrypted manners for an individual to receive their ePHI may include some types of text messaging, instant messaging, and other applications on a smartphone or another computing device that are capable of making an access request and receiving ePHI.[735] This exception for individual access requests under 45 CFR 164.524 would not apply when the individual would receive their ePHI using technology controlled by the regulated entity, such as a patient portal [736] or other technology for the transmission of ePHI (*e.g.,* API technology).[737] Such email or messaging technologies are considered to be among a covered entity's technology assets because they are components of a covered entity's relevant electronic information systems, and the requirement to encrypt ePHI would apply.

Under the right of access, an individual who is the subject of PHI has the right to inspect and request a copy of PHI about them in a designated record set, subject to certain exceptions. A regulated entity is required to provide such access in the form and format requested by the individual, if it is readily producible in such form and format. Thus, if an individual requests that the regulated entity provide them access in a manner that does not support encryption, a regulated entity is generally required to do so if it does not jeopardize the security of the regulated entity's information systems. For the exception to apply, a regulated entity would be required to have informed the individual of the risks associated with the transmission, receipt, and storage of unencrypted ePHI when the individual requests unencrypted access and to document that the individual has been informed of such risks.[738]

Consistent with the information blocking regulations, the information provided by regulated entities that are also actors must: focus on any current privacy and/or security risks posed by the technology or the third-party developer of the technology; be factually accurate, unbiased, objective, and not unfair or deceptive; and be provided in a non-discriminatory manner.[739] For example, a regulated entity that is an actor must provide information to individuals about the privacy and security risks of all mobile health applications in the same manner.

We are not proposing to require that the documentation be in any particular form or format. Rather, the required information could be on a standard form, chart note, or checkbox, as examples. The Department does not propose to apply this exception to ePHI transmitted in other forms or formats, such as on a CD or other physical device used to maintain and transmit ePHI. The proposal would not absolve a regulated entity from compliance with other applicable laws or regulations, including the information blocking regulations.[740]

We recognize that emergencies or other occurrences may render it infeasible to encrypt ePHI. Thus, the third proposed exception at 45 CFR 164.312(b)(3)(iii) would apply to certain circumstances in which encryption is infeasible. Such circumstances would be limited to when there is emergency or other occurrence that adversely affects a regulated entity's relevant electronic information systems. For the proposed exception to apply, a regulated entity would be required to implement reasonable and appropriate compensating controls in accordance with and determined by its contingency plan.[741] The Department would expect this proposed exception to be applicable for a limited period of time and only when encryption is infeasible. As noted above, the proposed exception to encryption would narrowly apply only when a regulated entity's relevant electronic information system is adversely affected by the emergency or other occurrence. The proposed exception would no longer be applicable at such time encryption becomes feasible, regardless of whether the emergency or other occurrence continues.

The fourth proposed set of exceptions at proposed 45 CFR 164.312(b)(3)(iv) would be for ePHI that is created, received, maintained, or transmitted by a medical device (*i.e.,* a ''device'' within the meaning of section 201(h) of the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. 321(h)) that is authorized by the FDA for marketing. We propose three separate exceptions for devices that are authorized by the FDA for marketing pursuant to: a submission received before March 29, 2023; a submission received on or after March 29, 2023, where the device is no longer supported by its manufacturer; or a submission received on or after March 29, 2023, where the device is supported by its manufacturer. Where a device has been authorized by the FDA for marketing pursuant to a submission received before March 29, 2023, we propose that the exception at proposed 45 CFR 164.312(b)(3)(iv)(A) would be available only where the regulated entity deploys in a timely manner any updates or patches required or recommended by the manufacturer of the device. We also propose a similar exception at proposed 45 CFR 164.312(b)(3)(iv)(B) for devices authorized by the FDA for marketing pursuant to a submission received on or

[735] Messaging in the context of telehealth is discussed in Department guidance on telehealth. *See* ''Guidance on How the HIPAA Rules Permit Covered Health Care Providers and Health Plans to Use Remote Communication Technologies for Audio-Only Telehealth,'' Office for Civil Rights, U.S. Department of Health and Human Services (June 13, 2022), *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-audio-telehealth/index.html.*

[736] For example, health IT certified through the ONC Health IT Certification Program as meeting the ''[v]iew, download, and transmit to 3rd party'' certification criterion must be able to create and transmit continuity of care document summaries to patients through email via an encrypted method of electronic transmission. *See* 45 CFR 170.315(e)(1).

[737] The ONC Health IT Certification Program sets forth at 45 CFR 170.550(h) the privacy and security certification framework for Health IT Modules. Section 170.550(h) identifies a mandatory minimum set of the certification criteria that ONC ACBs must ensure are also included as part of specific Health IT Modules that are presented for certification. For example, to meet the ''[s]tandardized API for patient and population services'' certification criterion, the ONC Health IT Certification Program requires that a Health IT Module presented for testing and certification must demonstrate the ability to establish a secure and trusted connection with an application requesting data for patients. *See* 45 CFR 170.315(g)(10); *see also* 45 CFR 170.215.

[738] *See* ''Resource for Health Care Providers on Educating Patients about Privacy and Security Risks to Protected Health Information when Using Remote Communication Technologies for Telehealth,'' Office for Civil Rights, U.S. Department of Health and Human Services, (Oct. 17, 2023), *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/resource-health-care-providers-educating-patients/index.html.*

[739] *See* 45 CFR part 171; 85 FR 25642, 25815 (May 1, 2020).

[740] *See, e.g.,* 45 CFR part 171.

[741] 45 CFR 164.308(a)(13).

after March 29, 2023, where the device is no longer supported by its manufacturer, provided that the regulated entity has deployed any updates or patches required or recommended by the manufacturer.

We recognize that, to comply with this proposal, some regulated entities may incur costs for replacing legacy medical devices (*i.e.,* medical devices that cannot be reasonably protected against current cybersecurity threats).[742] We also recognize that legacy devices can pose significant risks to the confidentiality, integrity, and availability of ePHI.[743] By limiting these exceptions to devices that have been updated and/or patched while they were supported by their manufacturer, we believe that this proposal would balance the interest in encouraging regulated entities to dispense with legacy devices with the cost of replacing such devices. Additionally, the Department believes that regulated entities should already have plans to replace legacy devices that cannot be made cybersecure because of their existing Security Rule obligations. We also recognize that at some point, most, if not all, devices will likely become legacy devices and that there may be legitimate reasons not to immediately replace them when the manufacturer ceases to provide support. In such cases, it will continue to be important for regulated entities to plan for how to address their ongoing Security Rule obligations.

Finally, we propose an exception, proposed 45 CFR 164.312(b)(3)(iv)(C), that would be available for a device authorized by the FDA for marketing pursuant to a submission received on or after March 29, 2023, where the device is supported by its manufacturer. We understand that the FDA considers security during the review of medical device marketing submissions, including those for software that is approved as a medical device, and works with device manufacturers to ensure that appropriate cybersecurity protections are built into such devices, pursuant to FDA's authority under the Consolidated Appropriations Act, 2023.[744] Thus, we do not believe it would be necessary or appropriate for the Security Rule to require encryption for an FDA-authorized medical device that has been authorized by the FDA for marketing pursuant to a submission received on or after March 29, 2023 where the device continues to be supported by its manufacturer.

Where a proposed exception applies to the proposed encryption requirement, the Department also proposes to require that a regulated entity implement alternative measures and compensating controls. Specifically, we propose at proposed 45 CFR 164.312(b)(4)(i) to require a regulated entity to document the existence of an applicable exception and implement reasonable and appropriate compensating controls. Under the proposal, we would require documentation to occur in real-time, meaning when the criteria for the exception exist and at the time compensating controls are implemented. For example, a regulated entity disclosing ePHI to an individual by unencrypted email in accordance with the right of access would be required to document in accordance with the proposed 45 CFR 164.312(b)(4)(i) that: (1) before the disclosure, the individual has requested to receive ePHI by unencrypted email or unencrypted messaging technology; and (2) before the disclosure, the regulated entity informed the individual of the risks associated with transmission of unencrypted ePHI. The exception would not apply where such individual requests to receive access to their ePHI pursuant to 45 CFR 164.524 via email or messaging technologies implemented by the covered entity.

At proposed 45 CFR 164.312(b)(4)(i), the Department proposes to require that where a proposed exception applies, a regulated entity would also be required to implement an alternative measure or measures that are reasonable and appropriate compensating controls under proposed 45 CFR 164.312(b)(4)(ii). Compensating controls would be implemented in the place of encryption to protect ePHI from unauthorized access.[745] The Department does not propose to require that compensating controls be limited to technical controls. Rather, a regulated entity should consider the nature of the exception, operating environment, and other appropriate circumstances to determine what controls are reasonable and appropriate and implement compensating controls effective for those circumstances. For example, a regulated entity may use physical access controls, such as physically limiting access to a device, in combination with other controls to compensate for the absence of encryption.

Proposed paragraph (b)(4)(ii)(A) would require that if the regulated entity has determined that an exception applies, it must secure ePHI by implementing reasonable and appropriate compensating controls that are reviewed and approved by the regulated entity's designated Security Official. Because exceptions are a departure from the Security Rule framework, the Department proposes to ensure appropriate focus and review by the Security Official of the controls chosen to compensate for the absence of encryption.

With respect to the exception at proposed 45 CFR 164.312(b)(3)(iv)(C), the Department proposes at paragraph (b)(4)(ii)(B) to presume that a regulated entity had implemented reasonable and appropriate compensating controls where the regulated entity has deployed the security measures prescribed and as instructed by the FDA-authorized label for the device. This would include any updates, including patches recommended or required by the manufacturer of the device. The proposed language recognizes that while the device's label may not specifically require deployment of an encryption solution, it may provide for a specific compensating control and the manner in which that control is to be implemented. While not required, a regulated entity would be permitted to implement additional alternative security measures and compensating controls in accordance with best practices and/or its risk analysis.

Finally, at proposed paragraph (b)(4)(ii)(C), the Department proposes to require that the regulated entity's Security Official review and document the implementation and effectiveness of the compensating controls during any period in which such compensating controls are in use to continue securing ePHI and relevant electronic

[742] *See* ''Next Steps Toward Managing Legacy Medical Device Cybersecurity Risks,'' MITRE Corporation (Nov. 2023), *https://www.mitre.org/sites/default/files/2023-11/PR-23-3695-Managing-Legacy-Medical-Device%20Cybersecurity-Risks.pdf;* ''Principles and Practices for the Cybersecurity of Legacy Medical Devices,'' International Medical Device Regulators Forum, p. 8 (Apr. 11, 2023), *https://www.imdrf.org/sites/default/files/2023-04/IMDRF%20Principles%20and%20Practices%20of%20Cybersecurity%20for%20%20Legacy%20Medical%20Devices%20Final%20%28N70%29_1.pdf.*

[743] ''Cybersecurity,'' U.S. Food & Drug Administration, U.S. Department of Health and Human Services, *https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity.*

[744] *See* sec. 3305 of Public Law 117–328, 126 Stat. 5832 (Dec. 29, 2022) (codified at 21 U.S.C. 360n–2); *see also* ''Cybersecurity in Medical Devices Frequently Asked Questions (FAQs),'' U.S. Food & Drug Administration, U.S. Department of Health and Human Services, *https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faqs.*

[745] Celia Paulsen, et al., ''Glossary of Key Information Security Terms,'' NIST Interagency and Internal Reports 7298, Revision 3, National Institute of Standards and Technology, U.S. Department of Commerce (July 3, 2019), *https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf.*

information systems. While regulated entities should review deployed compensating controls on a routine basis, the Department proposes to require a regulated entity to periodically review the implementation and effectiveness of compensating controls to ensure the continued protection of ePHI.[746] For example, if a regulated entity's plan to migrate ePHI from hardware that does not support encryption changes such that the use of the unencrypted hardware continues for a longer period of time, the regulated entity should review implemented compensating controls to ensure ongoing effectiveness and whether new compensating controls should be deployed. We propose to require the designated Security Office conduct such review at least once every 12 months or in response to environmental or operational changes, whichever is more frequent. Additionally, the Department proposes to require that the review be documented in writing and signed. If the regulated entity's Security Official review determines that certain compensating controls are no longer effective, the Department expects that the regulated entity would adopt new compensating controls that are effective to continue to meet the applicable exception. For example, a regulated entity would be expected to update any compensating controls for use of an FDA-authorized medical device when and as instructed by the manufacturer of the device.

We also propose to add an implementation specification for maintenance at proposed 45 CFR 164.312(b)(5). Under this proposal, a regulated entity would be expressly required to review and test the effectiveness of the technical controls required by the standard for encryption at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate. This proposal is consistent with others in this NPRM that would require regulated entities to maintain specified administrative, physical, and technical safeguards.

[746] The Department does not propose to require that the periodic review include a review of whether the conditions of the exception continue to apply because, when the conditions qualifying for an exception change such that an exception no longer applies, a regulated entity would be expected to resume compliance with the standard for encryption and decryption and the associated implementation specifications without exception.

d. Section 164.312(c)(1)—Standard: Configuration Management

The Department believes that the failure to configure technical controls appropriately and to establish and maintain secure baselines for relevant electronic information systems and technology assets in its relevant electronic information systems presents an opportunity for cyberattack and compromise of ePHI.[747] Accordingly, we propose to add a standard for configuration management at proposed 45 CFR 164.312(c)(1). The proposed standard would require a regulated entity to establish and deploy technical controls for securing relevant electronic information systems and technology assets in its relevant electronic information systems, including workstations, in a consistent manner. Under this proposal, a regulated entity also would be required to establish a baseline (*i.e.,* minimum) level of security for each relevant electronic information system and technology asset in its relevant electronic information systems and to maintain such information systems and technology assets according to those secure baselines. Consistent with our proposals regarding risk analysis and risk management planning, the Department intends for a regulated entity to establish its security baseline and to maintain that baseline even when technology changes. For example, a regulated entity that uses software to access ePHI would be required to update the software with patches as reasonable and appropriate. But where a developer ceases to support a software, it would be reasonable and appropriate for the regulated entity to take steps to either replace it or to otherwise ensure that its level of security remains consistent with the regulated entity's established baseline. Under this proposal, if finalized, the Department would expect a regulated entity to continually monitor its relevant electronic information systems and technology assets in its relevant electronic information systems to ensure that the secure baselines established by the regulated entity are maintained and take appropriate actions when a relevant electronic information system or technology asset in a relevant electronic information system fails to meet the established baselines. A regulated entity's secure baselines would be determined based on its risk analysis and use of security settings that are consistent across its relevant electronic information systems and technology assets in its relevant electronic information systems. For example, the risk analysis may determine that a manufacturer's default settings for a particular technology asset are insufficient. Accordingly, the regulated entity may establish the baseline for settings that should be applied to the particular asset and similar technologies across the regulated entity's enterprise. This proposed standard aligns with the Department's enhanced CPG for Configuration Management, which calls for regulated entities to define secure device and system settings. It also aligns with the enhanced CPG for Detect and Respond to Relevant Threats and Tactics, Techniques, and Procedures by calling for regulated entities to include malware protection in their security baseline to detect threats and protect electronic information systems.[748] Additionally, the proposed standard also aligns with the Department's essential CPG for Email Security, which addresses the reduction of risks from email-based threats.[749]

The Department proposes five implementation specifications for the proposed standard for configuration management.[750] Under the proposed implementation specification for anti-malware protection at proposed 45 CFR 164.312(c)(2)(i), a regulated entity would be required to deploy technology assets and/or technical controls that protect all of the technology assets in its relevant electronic information systems against malicious software, such as viruses and ransomware. Anti-malware software, especially when used in combination with other technical controls such as intrusion detection/prevention solutions, can also help prevent, detect, and contain cyberattacks.[751] This protection would be applied to all of a regulated entity's technology assets in its relevant electronic information systems. When determining how to fulfill this proposed obligation, regulated entities may consider deploying tools such as anti-malware and endpoint detection and response (EDR) solutions. Anti-malware tools generally scan a regulated entity's electronic information systems to

[747] ''Defending Against Common Cyber-Attacks,'' *supra* note 396; *see also* ''HIPAA and Cybersecurity Authentication,'' *supra* note 368.

[748] ''Cybersecurity Performance Goals,'' *supra* note 18.

[749] *Id.*

[750] *See* proposed 45 CFR 164.312(c)(2).

[751] ''What Happened to My Data?: Update on Preventing, Mitigating and Responding to Ransomware,'' Cybersecurity Newsletter, Office for Civil Rights, U.S. Department of Health and Human Services (Dec. 2019), *https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-fall-2019/index.html.*

identify malicious software.[752] Such tools may also quarantine malicious software if identified. As explained by the Office of Management and Budget, ''EDR combines real-time continuous monitoring and collection of endpoint data [. . .] with rules-based automated response and analysis capabilities.'' [753]

We propose a new implementation specification for software removal at proposed 45 CFR 164.312(c)(2)(ii) to require a regulated entity to remove extraneous software from the regulated entity's relevant electronic information systems. Software is extraneous if it is unnecessary for the regulated entity's operations. It can be a target for attack, and older applications may no longer be supported with patches for new vulnerabilities.[754] Removal of unnecessary software reduces an avenue of attack. The Department is not proposing to specify what would constitute necessary and unnecessary software. Rather, we intend that the regulated entity would consider removal of unwanted or unused software, for example, default software added by a computer manufacturer or reseller where such software may open an avenue for unnecessary risk because the regulated entity does not intend to use it. Accordingly, the proposal would require a regulated entity to consider all software on its relevant electronic information systems and any potential avenue of risk and address the risk through software removal where such software is unnecessary for the regulated entity's operations.

The proposed implementation specification for configuration at proposed 45 CFR 164.312(c)(2)(iii) would require a regulated entity to configure and secure operating systems and software in a manner consistent with the regulated entity's risk analysis. Generally, a regulated entity's risk analysis should guide its implementation of appropriate technical controls to reduce the risk to ePHI.[755] Requiring operating systems and software to be maintained in a secure manner would reduce exploitable vulnerabilities.[756] Often, known vulnerabilities can be mitigated by applying vendor patches or upgrading to a newer version.[757]

Under the proposed implementation specification for network ports at proposed 45 CFR 164.312(c)(2)(iv), a regulated entity would be required to disable network ports in accordance with the regulated entity's risk analysis.[758] Successful ransomware deployment often depends on the exploitation of technical vulnerabilities such as unsecured ports.[759] The proposal to require network ports to be disabled in accordance with the risk analysis would reduce exploitable vulnerabilities.[760]

Lastly, the proposed implementation specification for maintenance at proposed 45 CFR 164.312(c)(2)(v) would expressly require a regulated entity to review and test the effectiveness of the technical controls required by the other implementation specifications associated with the standard for configuration management at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

e. Section 164.312(d)(1)—Standard: Audit Trail and System Log Controls

Audit controls are crucial technical safeguards that are useful for recording and examining activity in electronic information systems, especially when determining whether a security violation occurred.[761] A regulated entity must consider its risk analysis and organizational factors, such as current technical infrastructure, hardware, and software security capabilities, to determine reasonable and appropriate audit controls.[762] However, based on OCR's enforcement experience, we believe that regulated entities' understanding of and compliance with this standard could be improved by providing more specificity.

Accordingly, the Department proposes to redesignate the standard for audit controls at 45 CFR 164.312(b) as proposed 45 CFR 164.312(d)(1), rename it as the standard for audit trail and system log controls, and to add a paragraph heading to clarify the organization of the regulatory text. We also propose to modify it to require a regulated entity to deploy either or both technology assets and technical controls that record and identify activity in the regulated entity's relevant electronic information systems. The proposal would replace ''procedural mechanisms'' with ''technical controls,'' to match the general focus on technical controls in 45 CFR 164.312 and would recognize that a regulated entity may be able to meet the requirements of the standard by deploying either or both technology assets (*e.g.,* software) or technical controls. Under the proposal, a regulated entity would be required to collect sufficient information to understand what a specific activity in its relevant electronic information systems is, such that the regulated entity would be better able to address activity that presents a risk to the confidentiality, integrity, or availability of ePHI. For example, a regulated entity should understand that a given activity in a relevant electronic information system is an attempt to access a portable workstation without authorization. The proposal also would modify the limitation on the regulated entity's obligation to record and identify activity in its relevant electronic information systems. Thus, the proposal would require a regulated entity to record and identify any activity that could present a risk to ePHI, meaning activity in all of its relevant electronic information systems, not only in its electronic information systems that create, receive, maintain, or transmit ePHI. In so doing, the Department would also require a regulated entity to record and identify activity in its electronic information systems that may affect the confidentiality, integrity, or availability of ePHI. This redesignated standard, as proposed, aligns more closely with the Department's enhanced CPG for Centralized Log Collection by addressing the deployment of technical controls to record and identify activity in all electronic information systems.[763] Additionally, as an example, we note that adoption of health IT certified through the ONC Health IT Certification Program may contribute to a regulated entity's compliance with the proposed standard for audit trail and system log controls where such health IT meets the criteria for auditing actions on health information and recording actions related to electronic health information and audit log status.[764]

[752] *See* ''Understanding Anti-Virus Software,'' Cybersecurity & Infrastructure Security Agency, U.S. Dept. of Homeland Security (June 30, 2009, rev. Sept. 27, 2019), *https://www.cisa.gov/news-events/news/understanding-anti-virus-software.*

[753] ''Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response,'' M–22–01, Office of Management and Budget, Executive Office of the President, p. 1 (Oct. 8, 2021), *https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf.*

[754] ''Defending Against Common Cyber-Attacks,'' *supra* note 396.

[755] *Id.*

[756] *Id.*

[757] *Id.*

[758] *See* proposed 45 CFR 164.308(a)(2).

[759] ''What Happened to My Data?: Update on Preventing, Mitigating and Responding to Ransomware,'' *supra* note 751.

[760] ''Defending Against Common Cyber-Attacks,'' *supra* note 396.

[761] ''Security Standards: Technical Safeguards,'' *supra* note 343, p. 7.

[762] *Id.*

[763] ''Cybersecurity Performance Goals,'' *supra* note 18.

[764] The criterion for auditing actions on health information requires adoption of health IT that has

The Department proposes four implementation specifications under this proposed standard that are intended to improve the effectiveness of audit controls deployed by a regulated entity. The proposed implementation specification for monitoring and identifying activity at proposed 45 CFR 164.312(d)(2)(i) would require a regulated entity to deploy technology assets and/or technical controls that monitor in real-time (*i.e.,* contemporaneously) all activity occurring in a regulated entity's relevant electronic information systems and identify indications of unauthorized persons and unauthorized activity, as determined by the regulated entity's risk analysis. As proposed, the technology assets and/or technical controls also would be required to alert workforce members of such indications in accordance with the regulated entity's policies and procedures for information system activity review at proposed 45 CFR 164.308(a)(7). Unauthorized activity may include actions by technology assets or persons that have not been authorized to access the regulated entity's ePHI or relevant electronic information systems. It may also include actions by authorized users or technology assets that are inconsistent with the regulated entity's policies and procedures for information access management at proposed 45 CFR 164.308(a)(10). The Department proposes that monitoring be continual and conducted in real-time because asynchronous review would allow for the compromise of ePHI for the period of time between the unauthorized activity and its discovery. OCR's enforcement experience has shown that some regulated entities are potentially failing to implement appropriate audit controls or to review information system activity in a timely manner, which may have contributed to a reportable breach.[765]

A regulated entity would be required, under the proposed implementation specification for recording activity at proposed 45 CFR 164.312(d)(2)(ii), to deploy technology assets and/or technical controls that record in real-time all activity in the regulated entity's relevant electronic information systems.[766] While technical assets and/or technical controls deployed in accordance with proposed 45 CFR 164.312(d)(2)(i) would monitor activity in its relevant electronic information systems, recording such activity would enable a regulated entity to assess any activity to better understand the activity's effects. The proposed implementation specification at proposed 45 CFR 164.312(d)(2)(iii) would require a regulated entity to deploy technology assets and/or technical controls to retain records of all activity in its relevant electronic information systems as determined by the regulated entity's policies and procedures for information system activity review at 45 CFR 164.308(a)(7)(ii)(A). The proposed implementation specification for scope of activity at proposed 45 CFR 164.312(d)(2)(iv) would clarify what would constitute activity to be monitored and recorded in the regulated entity's relevant electronic information systems as required by the proposed implementation specifications at proposed 45 CFR 164.312(d)(2)(i) and (ii). Specifically, the Department proposes that such activities would include, but would not be limited to, creating, accessing, receiving, transmitting, modifying, copying, or deleting ePHI; and creating, accessing, receiving, transmitting, modifying, copying, or deleting relevant electronic information systems and the information (*i.e.,* not only ePHI) therein.

We also propose to add an implementation specification for maintenance at proposed 45 CFR 164.312(d)(2)(iv). Under this proposal, a regulated entity would be expressly required to review and test the effectiveness of the technology assets and/or technical controls required by the respective implementation specifications of this section at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

f. Section 164.312(e)—Standard: Integrity

Improper alteration or destruction of ePHI, even unintentionally, can result in clinical quality problems, including patient safety issues, for a covered entity.[767] Workforce members or business associates may make accidental or intentional changes that improperly alter or destroy ePHI.[768] Data can also be altered or destroyed without human intervention, such as by electronic media errors or failures.[769] It is important to protect ePHI from being compromised, regardless of the source.[770]

The current standard for integrity at 45 CFR 164.312(c)(1) requires implementation of policies and procedures, rather than actual deployment of technical controls, to ensure integrity of ePHI. To improve the effectiveness of this standard, the Department proposes to redesignate it as proposed 45 CFR 164.312(e) and modify it for clarity. Under the proposal, a regulated entity would be required to deploy technical controls to protect ePHI from improper alteration or destruction when at rest and in transit and to review and test the effectiveness of such technical controls at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate. For example, the adoption of health IT that is certified through the ONC Health IT Certification Program as having the technical capability to verify that the electronically exchanged health information contained within the health IT has not been altered, using a hashing algorithm that meets certain requirements, may contribute to a regulated entity's compliance with the proposed standard for integrity.[771] The Department proposes to remove the implementation specification at 45 CFR 164.312(c)(2) because technical controls to corroborate that ePHI has not been altered or destroyed in an unauthorized manner are commonly built into hardware and protocols today. Thus, it is unnecessary to require a regulated entity to specifically deploy such controls.

g. Section 164.312(f)(1)—Standard: Authentication

Authentication ensures that a person is in fact who they claim to be before being allowed access to ePHI by providing proof of identity.[772] The Department proposes to redesignate the standard for person or entity authentication at 45 CFR 164.312(d) as 45 CFR 164.312(f)(1) to rename it ''Authentication'' to reflect its broad purpose, and to add a paragraph heading to clarify the organization of the regulatory text. Additionally, consistent with our proposals to define

---

the technical capability to record actions related to electronic health information; restrict the ability for auditing to be disabled to a limited set of users, if the technology permits; detect whether an audit log has been altered; and not allow actions recorded related to electronic health information to be changed, overwritten, or deleted by technology. *See* 45 CFR 170.315(d)(10); *see* 45 CFR 170.315(d)(2); *see also* 45 CFR 170.210(e).

[765] *See, e.g.,* ''Montefiore Medical Center,'' *supra* note 248.

[766] *See* proposed 45 CFR 164.308(a)(2).

[767] ''Security Standards: Technical Safeguards,'' *supra* note 343, p. 8.

[768] *Id.*

[769] *Id.*

[770] *Id.*

[771] 45 CFR 170.315(d)(8).

[772] ''Security Standards: Technical Safeguards,'' *supra* note 343, p. 9.

''implement'' and ''deploy,'' we propose to replace the requirement for a regulated entity to implement procedures with a requirement to deploy technical controls. Also, consistent with our proposals to clarify that a regulated entity's obligations to ensure the confidentiality, integrity, and availability extend to all of its relevant electronic information systems, we propose to clarify that the regulated entity is to deploy technical controls to verify that a person seeking access to the regulated entity's relevant electronic information systems is the one claimed. The Department also proposes to modify the existing standard to clarify that a regulated entity would be required to deploy technical controls to verify that a technology asset seeking access to the regulated entity's relevant electronic information systems is the one claimed. Thus, the proposed standard for authentication would require a regulated entity to deploy technical controls to verify that a person or technology asset seeking access to ePHI and/or the regulated entity's relevant electronic information systems is, in fact, the person or technology asset that the person or asset claims to be. We also propose to remove the reference to an entity because entity is included within the definition of person.

The Department proposes four implementation specifications under this standard. Consistent with NCVHS' recommendation to eliminate the use of default passwords, the proposed implementation specification for information access management policies at proposed 45 CFR 164.312(f)(2)(i) would require a regulated entity to deploy technical controls in accordance with its information access management policies and procedures, including technical controls that require users to adopt unique passwords.[773] Among other things, this proposal would ensure that regulated entities change default passwords. Such unique passwords would be required to be consistent with current recommendations of authoritative sources. The Department does not propose to define authoritative sources and defers to best practices for setting and maintaining passwords of sufficient strength to ensure the confidentiality, integrity, and availability of ePHI. Under this proposal, a regulated entity would need to require its workforce members to change any default passwords to unique passwords that are consistent with current authoritative source recommendations for unique passwords, as well as prevent the sharing of passwords among workforce members. Default passwords, typically factory-set passwords, may be discovered in common product documentation and used by attackers to gain access to relevant electronic information systems.[774] Thus, the Department believes that it is crucial for the security of ePHI that a regulated entity eliminate the use of default passwords.

In addition to proposing the elimination of default passwords, the Department proposes a specific requirement for a regulated entity to deploy MFA in the implementation specification for MFA at proposed 45 CFR 164.312(f)(2)(ii). We propose to expressly require MFA, as recommended by NCVHS, because it increases security by ensuring that a compromise of a single credential does not allow access to unauthorized users.[775] MFA is an effective way to reduce the risk of brute force attacks and to increase the cost of such attack, making such an attack less appealing to intruders.[776] Further, deployment of MFA aligns with the Department's essential CPGs for Email Security and Multifactor Authentication because use of MFA would be applicable to email access and protect assets connected to the internet.[777] Accordingly, proposed 45 CFR 164.312(f)(2)(ii)(A) would require a regulated entity to deploy MFA to all technology assets in its relevant electronic information systems to verify that the person seeking access to its relevant electronic information system is the user that the person claims to be. A regulated entity should deploy MFA to all technology assets in its relevant electronic information systems in a manner consistent with its risk analysis. MFA allows for the use of different categories of factors as described earlier. A decision by a regulated entity to use specific factors during specific circumstances where MFA is deployed will be dependent upon the risks to ePHI identified by the regulated entity and the ability of technology to use such factors to authenticate specific users. For example, certain behavioral characteristics may not satisfy current standards for MFA; however, the Department anticipates that it may be reasonable and appropriate in the future for a regulated entity to adopt a solution where users provide such characteristics as one of the factors. Additionally, a regulated entity may identify varying levels of risk posed by its technology assets and elect to deploy MFA in different ways to address the risk posed by each asset. For example, consistent with its risk analysis, a regulated entity may choose to deploy a single sign-on (SSO) authentication solution using MFA to allow users to access multiple local applications, while also requiring users to authenticate using MFA to access certain cloud-based services.

This proposed implementation specification generally is consistent with ASTP/ONC's ''Health Data, Technology, and Interoperability: Patient Engagement, Information Sharing, and Public Health Interoperability'' (HTI–2) NPRM's proposed revisions to the MFA criterion requiring certified health IT to support authentication, through multiple elements, of the user's identity, according to today's standards such as those recommended by NIST, and enable user to configure, enable, and disable the MFA capabilities.[778] Adoption of health IT that is certified through the ONC Health IT Certification Program as meeting the proposed MFA criterion, should the proposal be finalized, may contribute to a regulated entity's compliance with the proposed implementation specification for MFA in this NPRM.

Under proposed 45 CFR 164.312(f)(2)(ii)(B), a regulated entity would be required to deploy MFA for any action that would change a user's privileges to the regulated entity's relevant electronic information systems in a manner that would alter the user's ability to affect the confidentiality, integrity, or availability of ePHI. These modified privileges may provide a user with a level of access inconsistent with a regulated entity's policies and procedures and increase the risk to ePHI by affording a user who does not need to have access to certain systems or information the opportunity to remove security measures deployed to protect ePHI. Because a user may affect the confidentiality, integrity, or availability of ePHI by accessing a relevant electronic information system, a regulated entity would be expected to

[773] Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123, p. 6.

[774] ''Risks of Default Passwords on the internet,'' Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security (Oct. 7, 2016), *https://www.cisa.gov/news-events/alerts/2013/06/24/risks-default-passwords-internet.*

[775] ''Multi-Factor Authentication,'' Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security (Jan. 5, 2022), *https://www.cisa.gov/sites/default/files/publications/MFA-Fact-Sheet-Jan22-508.pdf;* Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123, pp. 7–8.

[776] Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123, pp. 7–8.

[777] ''Cybersecurity Performance Goals,'' *supra* note 18.

[778] *See* 89 FR 63498, 63574, 63506, 63528 (Aug. 5, 2024) (proposed 45 CFR 170.315(d)(13)(ii) of ASTP/ONC's HTI–2 NPRM).

deploy MFA for changed privileges in both types of systems.

Similar to the proposed standard for encryption, the Department proposes three exceptions at proposed 45 CFR 164.312(f)(2)(iii) to the proposed specific requirement to implement MFA. The first proposed exception at proposed 45 CFR 164.312(f)(2)(iii)(A) would be for a technology asset that does not support MFA but is currently in use by a regulated entity. Because the requirements for authentication under the existing Security Rule today do not expressly refer to MFA, a regulated entity that is not using MFA to meet the requirement to authenticate user identities may argue that it is in compliance with the authentication standard without using MFA. The Department recognizes that it may take some time for a regulated entity to adopt compliant software or hardware, and thus we propose an exception where such software or hardware does not support MFA. To meet this exception, a regulated entity would be required to establish a written plan to migrate ePHI to technology assets that supports MFA and to actually migrate the ePHI to such technology assets in accordance with the written plan. Accordingly, a regulated entity would be required to establish the plan, implement the plan, and actually migrate ePHI to technology assets that supports MFA within a reasonable and appropriate period of time. For example, it would not be reasonable and appropriate for a regulated entity to establish a plan to migrate to a new practice management system that supports MFA and fail to take any steps to perform the migration for an entire year. Applying the standard flexibly and at scale, a reasonable and appropriate timeframe for a system with 5,000 users may be different than one for a solo practitioner; however, both entities would be expected to progress to completion.

We recognize that emergencies or other occurrences may render it infeasible for a regulated entity to use MFA, so we propose a second exception for when MFA is infeasible during an emergency or other occurrence that adversely affects the regulated entity's relevant electronic information systems or the confidentiality, integrity, or availability of ePHI.[779] For the proposed exception to apply, a regulated entity would be required to implement reasonable and appropriate compensating controls in accordance with its contingency plan[780] and emergency access procedures.[781] For example, if an optical scanner used by a regulated entity as one of the required factors for MFA is rendered inoperable (*e.g.,* is temporarily broken or adversely affected by a cyberattack), a compensating control may be to temporarily allow users to log in with their user name and a unique password, rather than with a PIN and retinal scan. The Department would make this proposed exception applicable only for the limited period of time in which MFA is infeasible for the regulated entity during the emergency or other occurrence, regardless of whether the emergency or other occurrence continues.

At proposed 45 CFR 164.312(f)(2)(iii)(C), we propose three exceptions that would be for a technology asset in use that is a device within the meaning of section 201(h) of the Food, Drug, and Cosmetic Act that has been authorized for marketing by the FDA. The first would be for a device authorized by the FDA for marketing pursuant to a submission received before March 29, 2023, while the second would be for a device authorized by the FDA for marketing pursuant to a submission received on or after March 29, 2023, that is no longer supported by its manufacturer. In both cases, the exception would only apply where, the regulated entity has deployed any updates or patches required or recommended by the manufacturer of the device. Similar to our proposal for exceptions to encryption at proposed 45 CFR 164.312(b)(3)(iv)(A) and (B), we recognize that some regulated entities may incur costs of replacing legacy devices because of the limitations on the proposed exception to MFA where a device was submitted to the FDA for authorization before March 29, 2023 or a device submitted for authorization on or after that date that is no longer supported by its manufacturer.[782] However, as discussed above, such devices can pose significant risks to the confidentiality, integrity, and availability of ePHI.[783] By limiting these exceptions to devices that have been updated and/or patched while they were supported by their manufacturer, we believe that this proposal would balance the interest in encouraging regulated entities to dispense with legacy devices with the cost of replacing such devices. Additionally, the Department believes that regulated entities should already have plans to replace legacy devices that cannot be made cybersecure because of their existing Security Rule obligations. As discussed above, we also recognize that at some point, most, if not all, devices will likely become legacy devices and that there may be legitimate reasons not to immediately replace them when the manufacturer ceases to provide support. In such cases, it will continue to be important for regulated entities to plan for how to address their ongoing Security Rule obligations.

The third proposed exception to MFA at 45 CFR 164.312(f)(2)(iii)(C)(*3*) for devices authorized by the FDA for marketing would be available for those devices authorized for marketing by the FDA pursuant to a submission received on or after March 29, 2023, where they are supported by their manufacturer. We understand that the FDA considers security during the review of medical device marketing submissions and works with device manufacturers to ensure that appropriate cybersecurity protections are built into such devices, pursuant to FDA's authority under the Consolidated Appropriations Act, 2023.[784] Thus, we do not believe it would be necessary or appropriate for the Security Rule to require MFA for an FDA-authorized medical device that has been authorized by FDA for marketing pursuant to a submission received on or after March 29, 2023, where the device continues to be supported by its manufacturer. However, these devices may continue to be used by a regulated entity when they are no longer supported, consistent with the proposed exception for legacy devices that were approved pursuant to a submission received on or after March 29, 2023, as described above.

Where a proposed exception would apply to the proposed MFA requirement, the Department proposes to require that a regulated entity implement alternative measures and compensating controls.[785] Specifically, when a regulated entity seeks to comply with the Security Rule by meeting one of the proposed exceptions to the proposed MFA requirement, the Department proposes to require a regulated entity to document both the existence of the criteria demonstrating that the proposed exception would apply and the rationale for why the proposed exception would apply.

[779] *See* proposed 45 CFR 164.312(f)(2)(iii)(B).

[780] *See* proposed 45 CFR 164.308(a)(13).

[781] *See* proposed 45 CFR 164.312(a)(2)(iii).

[782] *See* ''Next Steps Toward Managing Legacy Medical Device Cybersecurity Risks,'' *supra* note 742; ''Principles and Practices for the Cybersecurity of Legacy Medical Devices,'' *supra* note 742, p. 8.

[783] ''Cybersecurity,'' *supra* note 743.

[784] *See* sec. 3305 of Public Law 117–328, 126 Stat. 5832 (Dec. 29, 2022) (codified at 21 U.S.C. 360n–2); *see also* ''Cybersecurity in Medical Devices Frequently Asked Questions (FAQs),'' *supra* note 744.

[785] Proposed 45 CFR 164.312(f)(2)(iv)(A).

Additionally, the proposal would require a regulated entity to implement reasonable and appropriate compensating controls, as described at proposed paragraph (f)(2)(iv)(B).

The proposed requirements for reasonable and appropriate compensating controls are explained under proposed 45 CFR 164.312(f)(2)(iv)(B). Compensating controls are implemented in the place of MFA to protect ePHI.[786] The Department does not propose to require that compensating controls be technical controls. Rather, a regulated entity should consider the nature of the exception, operating environment, and other appropriate circumstances to determine what controls are reasonable and appropriate and implement compensating controls effective for those circumstances. For example, if a software program does not support MFA, deploying a firewall or increasing the sensitivity of an existing firewall protecting that software may in some circumstances constitute a reasonable and appropriate compensating control.[787] In some instances, physical safeguards may serve as reasonable and appropriate compensating controls. For example, limiting access to certain components of a relevant electronic information system to workforce members who meet certain requirements may be a reasonable and appropriate compensating control under some circumstances. In most cases, it would be reasonable and appropriate for a regulated entity to implement multiple compensating controls to ensure that the affected electronic information system is secured.

The Department proposes at proposed 45 CFR 164.312(f)(2)(iv)(B)(*1*) that, to comply with an exception at paragraph (f)(2)(iii)(A) or (B) or (f)(2)(iii)(C)(*1*) or (*2*), the regulated entity would be required to secure the relevant electronic information system with reasonable and appropriate compensating controls that have been reviewed, approved, and signed by the regulated entity's Security Official. Because exceptions are a departure from the designed Security Rule framework, the Department intends to ensure appropriate review by the Security Official of controls selected by the regulated entity to compensate for the absence of MFA. Merely because a regulated entity's Security Official has reviewed, approved, and signed off on compensating controls does not mean that those controls are effective. The regulated entity would also be required to give due consideration to the circumstances surrounding the exception and implement compensating controls effective for those specific circumstances.

With respect to the exception at proposed 45 CFR 164.312(f)(2)(iii)(C)(*3*), the Department proposes at proposed 45 CFR 164.312(f)(2)(iv)(B)(*2*) to presume that a regulated entity had implemented reasonable and appropriate compensating controls where the regulated entity has implemented the security measures prescribed and as instructed by the FDA-authorized label for the device. The proposed language recognizes that while the device's label may not specifically require deployment of an MFA solution, it may provide for a specific compensating control and the manner in which that control is to be implemented. This would include any updates, such as patches, recommended or required by the manufacturer of the device. While not required, a regulated entity would be permitted to implement additional alternative security measures and compensating controls in accordance with best practices and/or its risk analysis.

Additionally, the Department proposes at 45 CFR 164.312(f)(2)(iv)(B)(*3*) that during any period in which compensating controls are in use, the regulated entity's Security Official would be required to review the effectiveness of the compensating controls at securing its relevant electronic information systems. While regulated entities should review implemented compensating controls on a routine basis, the Department intends for a regulated entity to periodically review the implementation and effectiveness of implemented compensating controls to ensure the continued protection of ePHI.[788] For example, if a regulated entity's plan to migrate ePHI from hardware that does not support MFA changes such that the use of the non-MFA hardware continues for a longer period of time, the regulated entity should review implemented compensating controls to ensure ongoing effectiveness and whether new compensating controls should be implemented. We are proposing to require that the review be conducted at least once every 12 months or in response to an environmental or operational change, whichever is more frequent, and that the review be documented. Additionally, the Department proposes to require that the review be documented. If the regulated entity's Security Official review determines that certain compensating controls are no longer effective, the Department would expect the regulated entity to adopt other compensating controls that are effective to continue to meet the applicable proposed exception.

As an example of how proposed 45 CFR 164.312(f)(2)(iii) would operate in concert with proposed 45 CFR 164.312(f)(2)(iv), a regulated entity experiencing an emergency that adversely affects a relevant electronic information system and renders MFA infeasible would be required to document the following:

- The regulated entity has experienced an emergency that has adversely affected a relevant electronic information system, including the nature of the emergency and the specific circumstances that adversely affected the specific electronic information system.
- MFA has been rendered infeasible with respect to the specific relevant electronic information system adversely affected by the emergency.
- The regulated entity has put in place reasonable and appropriate compensating controls in accordance with the regulated entity's emergency access procedures and contingency plan.

As part of its documentation, a regulated entity would need to include the controls that have been deployed, a record of the fact that the compensating controls are in use, and a record indicating that the compensating controls have been reviewed and approved by the regulated entity's Security Official. Proposed 45 CFR 164.312(f)(2)(iv)(B)(*3*) would require the Security Official to review and document the effectiveness of the compensating controls at least once every 12 months or in response to an environmental or operational change, whichever is more frequent. A determination regarding the effectiveness of the technical controls would be based on their ability to secure the regulated entity's ePHI and its relevant electronic information systems.

Last, we propose to add an implementation specification for maintenance at proposed 45 CFR 164.312(f)(2)(v). Under this proposal, a regulated entity would be expressly required to review and test the effectiveness of the technical controls required by this standard at least once every 12 months or in response to

[786] ''Glossary of Key Information Security Terms,'' *supra* note 745.

[787] ''Securing Your Legacy [System Security],'' *supra* note 494.

[788] The Department does not propose that the periodic review include a review that the conditions of the exception continue to apply because a regulated entity would be expected to resume compliance with the implementation specification of multi-factor authentication when such exception no longer applies.

environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

h. Section 164.312(g)—Standard: Transmission Security

Transmission security protects against the interception of ePHI in the communications networks used by regulated entities to transmit ePHI.[789] The Department proposes to redesignate the standard for transmission security as proposed 45 CFR 164.312(g) and to modify the standard consistent with other proposals made elsewhere in this NPRM, as described below. Specifically, we propose to clarify the existing standard by requiring a regulated entity to deploy technical controls to guard against unauthorized access to ePHI in transmission over an electronic communications network. For example, adoption of health IT that is certified through the ONC Health IT Certification Program as having the technical capability to establish a trusted connection using encrypted and integrity message protection or a trusted connection for transport and deploying such capability may contribute to a regulated entity's compliance with the proposed standard for transmission security.[790] These proposed changes are consistent with the Department's proposals to replace ''implement'' with ''deploy'' in the context of technical safeguards to differentiate between implementation of a written policy or procedure and deployment of technical controls.

Consistent with our proposals to require that regulated entities maintain their technical controls, we also propose to require a regulated entity to review and test the effectiveness of its technical controls for guarding against unauthorized access to ePHI that is being transmitted over an electronic communications network. We propose that such review and testing occur at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify such technical controls as reasonable and appropriate.

The Department also proposes to remove the implementation specification for integrity controls at 45 CFR 164.312(e)(2)(i) because these requirements are incorporated in the standard for integrity at proposed 45 CFR 164.312(e), discussed above. A regulated entity would continue to be required to review the current methods used to transmit ePHI and then deploy appropriate solutions to protect ePHI from improper alteration or destruction.[791]

i. Section 164.312(h)(1)—Standard: Vulnerability Management

Hackers can penetrate a regulated entity's network and gain access to ePHI by exploiting publicly known vulnerabilities.[792] Exploitable vulnerabilities can exist in many parts of the technology infrastructure of a regulated entity's relevant electronic information systems (*e.g.,* server, desktop, and mobile device operating systems; application, database, and web software; router, firewall, and other device firmware).[793] A regulated entity can identify technical vulnerabilities in multiple, complementary ways, including:

- Subscribing to CISA alerts[794] and bulletins.[795]
- Subscribing to alerts from the HHS Health Sector Cybersecurity Coordination Center.[796]
- Participating in an information sharing and analysis center (ISAC) or information sharing and analysis organization (ISAO).
- Implementing a vulnerability management program that includes using a vulnerability scanner to detect vulnerabilities such as obsolete software and missing patches.
- Periodically conducting penetration tests to identify weaknesses that could be exploited by an attacker.

Additionally, CISA has compiled a database of free cybersecurity services and tools, some provided directly by CISA and others provided by private and public sector organizations.[797] For example, public and private critical infrastructure organizations may avail themselves of CISA's Cyber Hygiene Services.[798] These services are available at no cost to such organizations and can help regulated entities reduce their risk level, identify vulnerabilities that could otherwise go unmanaged and increase the accuracy and effectiveness of their response activities, among other benefits, putting them in a better place to make risk-informed decisions. CISA's Cyber Hygiene Services include both vulnerability scanning and web application scanning. CISA also has compiled a specific suite of tools and services for high-risk communities.[799]

To address the potential for a bad actor to exploit publicly known vulnerabilities, and consistent with NCVHS' recommendation, the Department proposes to add a new standard for vulnerability management at 45 CFR 164.312(h)(1).[800] The proposed standard would require a regulated entity to deploy technical controls to identify and address technical vulnerabilities in the regulated entity's relevant electronic information systems. The deployment of technical controls should be consistent with the regulated entity's patch management policies and procedures at proposed 45 CFR 164.308(a)(4). This proposed standard aligns with the Department's enhanced CPGs for Cybersecurity Testing and Third Party Vulnerability Disclosure by calling for regulated entities to employ multiple processes to discover technical vulnerabilities, including vulnerabilities in workstations and in technology assets provided by vendors and service providers.[801] For example, a regulated entity should include a device owned by a person other than the regulated entity (*e.g.,* the medical device manufacturer) in its vulnerability management activities where the device is deployed on the regulated entity's network. The regulated entity should also include all workstations (*e.g.,* desktop computers, mobile devices) that are part of its relevant electronic information systems in its vulnerability management activities.

To implement this proposed standard, we propose four implementation specifications. Proposed 45 CFR 164.312(h)(2)(i)(A) would require a regulated entity to conduct automated scans of the regulated entity's relevant electronic information systems, including all of the components of such relevant electronic information systems (*e.g.,* workstations, private networks) to identify technical vulnerabilities. Vulnerability scans detect vulnerabilities such as obsolete software

[789] ''Glossary of Key Information Security Terms,'' *supra* note 745.

[790] *See* 45 CFR 170.315(d)(9).

[791] ''Security Standards: Technical Safeguards,'' *supra* note 343, p. 10–11.

[792] ''Defending Against Common Cyber-Attacks,'' *supra* note 396.

[793] *Id.*

[794] *See* ''Cybersecurity Alerts & Advisories,'' Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security, *https://www.cisa.gov/news-events/cybersecurity-advisories.*

[795] *See* ''Bulletins,'' Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security, *https://www.cisa.gov/news-events/bulletins.*

[796] *See* ''Health Sector Cybersecurity Coordination Center (HC3),'' Office of the Chief Information Officer, U.S. Department of Health and Human Services, *https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html.*

[797] ''Free Cybersecurity Services and Tools,'' *supra* note 313.

[798] ''Cyber Hygiene Services,'' *supra* note 313.

[799] ''Cybersecurity Resources for High-Risk Communities,'' *supra* note 313.

[800] Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123, p. 8–9.

[801] ''Cybersecurity Performance Goals,'' *supra* note 18.

and missing patches.[802] Once identified, assessed, and prioritized, appropriate measures need to be implemented to mitigate these vulnerabilities (*e.g.,* apply patches, harden systems, retire equipment).[803] Under the proposal, the scans would be required to be conducted in accordance with the regulated entity's risk analysis under proposed 45 CFR 164.308(a)(2) and no less frequently than once every six months.

Relatedly, proposed 45 CFR 164.312(h)(2)(i)(B) would add an implementation specification for maintenance of the technology assets that conduct the required automated vulnerability scans. Under this proposal, a regulated entity would be expressly required to review and test the effectiveness of the technology asset(s) that conducts the automated vulnerability scans that would be required by the proposed implementation specification at proposed 45 CFR 164.312(h)(2)(i)(A) at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

Identification of a known vulnerability in a relevant electronic information system or a component thereof is a necessary precursor for a regulated entity to take action to mitigate the vulnerability. A 2019 study on vulnerability and patch management found that 48 percent of respondents reported that their organizations had at least one breach in the preceding two years. Of those, 60 percent said that the breaches could have occurred because an available patch for a known vulnerability had not been applied.[804]

Accordingly, the Department also proposes a new implementation specification for monitoring at proposed 45 CFR 164.312(h)(2)(ii) to require that a regulated entity monitor authoritative sources for known vulnerabilities on an ongoing basis and take action to remediate identified vulnerabilities in accordance with the regulated entity's patch management program.[805] The Department expects such monitoring to be conducted on an ongoing basis and is not proposing to specify a minimum time interval for reviewing sources. We are also not proposing to prescribe the specific sources of known vulnerabilities because such sources may change over time and the vulnerabilities for which regulated entities may be monitoring may vary greatly among regulated entities. We propose to require that the sources used must be authoritative. Examples of authoritative sources of known vulnerabilities would include NIST's National Vulnerability Database [806] and CISA's Known Exploited Vulnerabilities Catalog.[807]

The proposed implementation specification for penetration testing at 45 CFR 164.312(h)(2)(iii) would require a regulated entity to conduct periodic testing of the regulated entity's relevant electronic information systems for vulnerabilities, commonly referred to as penetration testing. Penetration tests identify vulnerabilities in the security features of an application, system, or network by mimicking real-world attacks [808] and are an effective way to identify weaknesses that could be exploited by an attacker.[809] The proposal would require such testing to be conducted by qualified person(s). We propose to describe a qualified person as a person with appropriate knowledge of and experience with generally accepted cybersecurity principles and methods for ensuring the confidentiality, integrity, and availability of ePHI. We believe that within the cybersecurity industry, it is understood that a person who is qualified to conduct such penetration testing is an individual who has a combination of one or more qualifying credentials, skills, or experiences to perform ''ethical hacking'' or ''offensive security'' of information systems. The proposal would require a regulated entity to conduct such testing at least once every 12 months, or in accordance with the regulated entity's risk analysis,[810] whichever is more frequent.

Lastly, we are proposing a new implementation specification for patch and update installation at 45 CFR 164.312(h)(2)(iv) to require a regulated entity to configure and implement technical controls to install software patches and critical updates in a timely manner in accordance with the regulated entity's patch management program.[811] The proposed standard for patch management, an administrative safeguard discussed above, would require a regulated entity to establish and implement written policies and procedures for applying patches and updating relevant electronic information system configurations, while this proposal would require the regulated entity to implement technical controls to implement those written policies and procedures. In other words, proposed 45 CFR 164.312(h)(2)(iv) addresses the technical controls to effectuate a regulated entity's patch management plan. Applying patches for technology assets, including workstations, is an effective mechanism to mitigate known vulnerabilities and limit the risk of exploitation.[812] Although older applications or devices may no longer be supported with patches for new vulnerabilities, regulated entities still must take appropriate action if a newly discovered vulnerability affects an older application or device. If an obsolete, unsupported system cannot be upgraded or replaced, additional safeguards should be implemented or existing safeguards enhanced to mitigate known vulnerabilities until upgrade or replacement can occur (*e.g.,* increase access restrictions, remove or restrict network access, disable unnecessary features or services).[813] Deployment of such technical controls would help to ensure that a regulated entity's relevant electronic information systems are updated as quickly as possible after a vulnerability has been identified and a patch released.

The proposed standard for patch management, discussed above, would work in tandem with the proposed standard for vulnerability management to ensure that regulated entities substantially reduce the risk to ePHI from known vulnerabilities.[814] Together, these proposals would clarify that a regulated entity is required to affirmatively seek out information about known vulnerabilities, assess the risks to the confidentiality, integrity, and availability of ePHI, and implement effective mechanisms through both policies and procedures and technical controls to reduce the risk, as well the actual occurrence, of breaches resulting from known vulnerabilities. For example, known vulnerabilities should be readily identified by a regulated entity through monitoring of

[802] ''Defending Against Common Cyber-Attacks,'' *supra* note 396.

[803] *Id.*

[804] This study is not specific to health care. ''Costs and Consequences of Gaps in Vulnerability Response,'' ServiceNow and Ponemon Institute, p. 3 (2019), *https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf.*

[805] *See* proposed 45 CFR 164.308(a)(4).

[806] ''National Vulnerability Database,'' *supra* note 398.

[807] ''Known Exploited Vulnerabilities Catalog,'' *supra* note 399.

[808] ''Glossary of Key Information Security Terms,'' *supra* note 745.

[809] ''Defending Against Common Cyber-Attacks,'' *supra* note 396.

[810] *See* proposed 45 CFR 164.308(a)(2).

[811] *See* proposed 45 CFR 164.308(a)(5).

[812] ''Defending Against Common Cyber-Attacks,'' *supra* note 396.

[813] *See* ''Securing Your Legacy [System Security],'' *supra* note 494.

[814] *See* proposed 45 CFR 164.308(a)(5) and 164.312(h)(1).

authoritative sources for known vulnerabilities, such as those referenced above, and remediating any identified vulnerabilities. When a vulnerability is discovered, a regulated entity, through its patch management program, should have in place a policy and procedure for applying any available patches or implementing reasonable and appropriate compensating controls if a patch is not available. Remediation may be as simple as applying a vendor-offered software patch or, in the case of software no longer supported by a vendor, designing and implementing reasonable and appropriate compensating controls to reduce the risk of the vulnerability. The policies and procedures required by the proposed standard for patch management in proposed 45 CFR 164.308(a)(4)(i) also would be implemented in part by the proposed implementation specifications associated with the proposed standard for vulnerability management. Those proposed implementation specifications would require the deployment of technical controls to ensure the patch management program is carried out, automated vulnerability scans, and penetration testing, all of which may identify when a patch or compensating control has not been put in place. The Department envisions that the full implementation of all of the proposed standards and implementation specifications would effectively reduce the risk to ePHI.

j. Section 164.312(i)(1)—Standard: Data Backup and Recovery

The Security Rule requires regulated entities to regularly create copies of ePHI to ensure that it can be restored in the event of a loss or disruption.[815] However, OCR's enforcement experience indicates that regulated entities could benefit from a more specific standard. Consistent with the proposed standard for contingency planning at 45 CFR 164.308(a)(13)(ii)(B), the Department proposes to add a standard for a new technical safeguard for data backup and recovery. This new standard would require a regulated entity to deploy technical controls to create and maintain exact retrievable copies of ePHI. The proposed changes would remove the existing implementation specification for this activity from the physical safeguards section and place it within technical safeguards. The Department also proposes to modify the language of the existing requirement by removing the limitation that it applies before moving equipment, so that it applies broadly and comprehensively. Elevating data backup and recovery to a standard would also increase the prominence of this requirement and highlight the liability of regulated entities for creating the capacity to restore systems after a data breach.

The Department proposes four new implementation specifications for the data backup and recovery standard. The first, 45 CFR 164.312(i)(2)(i), would require a regulated entity to create copies of ePHI in a manner that ensures that such copies are no more than 48 hours older than the ePHI maintained in the regulated entity's relevant electronic information systems and in accordance with the policies and procedures required by proposed 45 CFR 164.308(a)(13)(ii)(B). The second, 45 CFR 164.312(i)(2)(ii), would require a regulated entity to deploy technical controls that, in real-time, monitor, and alert workforce members about, any failures and error conditions of the backups required by the first implementation specification. The third, 45 CFR 164.312(i)(2)(iii), would require a regulated entity to deploy technical controls that record the success, failure, and any error conditions of backups required. The fourth, 45 CFR 164.312(i)(2)(iv), would require a regulated entity to test the effectiveness of its backups and document the results at least monthly. Specifically, a regulated entity would be required to restore a representative sample of backed up ePHI (after the ePHI is backed up as required by paragraph (i)(2)(i)) and document the results of such test restorations at least monthly. Such tests should include verifying regulated entity's ability to access ePHI from a remote location.

These activities are included in NIST guidance for Security Rule compliance,[816] which directs regulated entities to consider the following questions: Is the frequency of backups appropriate for the environment? Are backup logs reviewed and data restoration tests conducted to ensure the integrity of data backups? Is at least one copy of the data backup stored offline to protect against corruption due to ransomware or other similar attacks? The potential need for these requirements also has been indicated through the rising number of ransomware attacks and the high number of individuals affected in such incidents. The Department believes these new implementation specifications, if finalized, would provide additional instruction for regulated entities about conducting data backups and enhance the ability of regulated entities to avoid costly work stoppages and interruptions in the delivery of health care when data becomes unavailable because of a disaster, security incident, or other emergency. We believe enhanced measures for data backup would reduce the need to pay ransom to hackers to recover compromised data.

k. Section 164.312(j)—Standard: Information Systems Backup and Recovery

The Department also proposes to add a new standard for backup and recovery of relevant electronic information systems at proposed 45 CFR 164.312(j). This proposed standard would require a regulated entity to deploy technical controls to create and maintain backups of relevant electronic information systems. It would also require a regulated entity to review and test the effectiveness of such technical controls at least once every six months or in response to environmental or operational changes, whichever is more frequent, and modify them as reasonable and appropriate. The Department would not require a regulated entity to test every relevant electronic information system; rather, the requirement to test the effectiveness of the controls would permit a regulated entity to review the relevant log files and to test a representative sample of the backup of its relevant electronic information systems.

This proposed standard would reduce potential gaps in the data that needs to be backed up and recovered, to ensure that regulated entities address compliance across relevant electronic information systems. It is crucial to a regulated entity's recovery from an emergency or other occurrence, including a security incident, that adversely affects its relevant electronic information systems to create and maintain backups of such information systems that comprise the infrastructure that maintains and supports the confidentiality, integrity, and availability of ePHI. The Department would expect that the extent of this activity would be affected by the size and complexity of the relevant electronic information systems used by a regulated entity. It is also consistent with NIST guidance, which directs regulated entities to consider whether backups or images of operating systems, devices, software, and configuration files necessary to support the

[815] *See* "Plan A . . . B . . . Contingency Plan!," *supra* note 606.

[816] *See* "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide," *supra* note 461, p. 49.

confidentiality, integrity, and availability of ePHI.[817]

4. Request for Comment

The Department requests comments on the foregoing proposals, including any benefits, drawbacks, or unintended consequences. We also request comment on the following considerations in particular:

a. Whether there are additional technical safeguards that the Department should require regulated entities to implement.

b. Whether there are additional implementation specifications that should be adopted for any of the proposed or existing technical safeguards.

c. Whether the Department should extend the standard for encryption and decryption and associated implementation specifications to require encryption of all relevant electronic information systems.

d. Whether there should be exceptions to any of the proposed or existing technical safeguards or related implementation specifications, in addition to those proposed for encryption and decryption and MFA. For example, are there any proposed or existing standards or implementation specifications with which small or rural regulated entities would have substantial difficulty complying? If so, please explain the type of regulated entities that would be adversely affected by the requirement, the nature of the compliance difficulty, and any alternative or compensating measures that such entities are implementing now or could implement in the event of such requirement to address the risk to ePHI posed by the specific standard or implementation specification.

e. Whether the exceptions the Department has proposed to the standard for encryption or decryption are appropriate. If not, please explain.

f. Data about the frequency and number of requests regulated entities receive pursuant to the individual right of access at 45 CFR 164.524 where an individual requests that the regulated entity transmit to the individual or a third party a copy of the individual's ePHI via unencrypted email or other unencrypted messaging technologies. Please confirm that these are requests made pursuant to the individual right of access, rather than other types of communications, such as appointment reminders or requests made pursuant to a valid authorization.

g. Whether the Department should provide any additional exceptions to standard for encryption or decryption. If so, please explain.

h. Whether there are additional criteria or parameters for encryption that regulated entities would find helpful. If yes, please explain and provide examples.

i. Whether the Department should require review of compensating controls implemented to comply with an exception to the encryption and decryption standard more frequently than once every 12 months where there are no environmental or operational changes.

j. With respect to the exception to the standard for encryption and decryption for certain requests made pursuant to the individual right of access, whether there are forms and formats the Department should include or exclude from the exception (*e.g.,* portable document format (PDF)). If so, please explain.

k. Resources that regulated entities have identified to help inform individuals about the risks associated with the unencrypted transmission of ePHI, and whether the Department should compile and publish a list of such resources.

l. Whether the Department should define in regulation or guidance what constitutes a prevailing cryptographic standard. If so, please explain.

m. Whether the Department should specify the deployment of a particular form or manner of encryption, such as the use of particular algorithms, protocols, or compliance standards. If so, please explain.

n. Whether the Department should specify how much time regulated entities have to implement encryption for technology assets that do not support encryption. If so, please explain.

o. Whether the Department should provide more detailed requirements for network segmentation, such as the type(s) of technologies that should be segmented and how to determine whether certain technologies should be segmented. If so, please explain.

p. Whether the exceptions the Department has proposed to the implementation specification for MFA are appropriate. If not, please explain.

q. Whether the Department should provide additional exceptions to the implementation specification for MFA. If so, please explain.

r. Whether the Department should require a regulated entity to review its compensating controls adopted to comply with the exceptions to the implementation specification for MFA more frequently than once every 12 months.

s. The costs and burdens for regulated entities to implement MFA.

t. Whether the Department should require regulated entities to deploy an endpoint detection and response (EDR), security information and event management (SIEM), or other specific solution.

u. Whether once every six months is the appropriate frequency for the automated vulnerability scans required under the implementation specification for vulnerability management. If not, please explain.

v. Whether the Department should define in regulation or guidance what constitutes an authoritative source of known vulnerabilities. If so, please explain.

w. Whether once every 12 months is the appropriate frequency for the penetration testing required under the implementation specification for vulnerability management. If not, please explain.

x. For regulated entities that have conducted penetration tests, the amount of time and costs of such tests.

G. Section 164.314—Organizational Requirements

1. Section 164.314(a)(1)—Standard: Business Associate Contracts or Other Arrangements

a. Current Provisions

The first standard in 45 CFR 164.314 contains the requirements for business associate agreements and other arrangements. The associated implementation specifications at 45 CFR 164.314(a)(2) require that a business associate agreement include provisions compelling a business associate to do all of the following: (1) comply with the requirements of the Security Rule;[818] (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 the Security Rule by also entering into a business associate agreement;[819] and (3) report to the covered entity any security incident of which it becomes aware, including breaches of unsecured PHI as required by the Breach Notification Rule.[820]

Under 45 CFR 164.314(a)(2)(ii), a covered entity that is a governmental entity is in compliance with the requirements of this section if it has in place an arrangement with a business associate that is also a governmental entity where the arrangement meets the

[817] *Id.*

[818] 45 CFR 164.314(a)(2)(i)(A).

[819] 45 CFR 164.314(a)(2)(i)(B).

[820] 45 CFR 164.314(a)(2)(i)(C).

analogous requirements of the Privacy Rule at 45 CFR 164.504(e)(3).[821]

Additionally, 45 CFR 164.314(a)(2)(iii) requires that a business associate and its subcontractor enter into a business associate agreement that meets the same requirements as those that apply to a business associate agreement between a covered entity and business associate.

As described above, a business associate agreement must include a provision that requires a business associate to report to the covered entity any known security incident. The term ''security incident'' includes both attempted and successful unauthorized events in an information system.[822] The Security Rule does not prescribe the timing and frequency with which a business associate reports a security incident to the covered entity (or subcontractor to a business associate).[823] Instead, regulated entities may determine the appropriate timing and frequency as part of their business associate agreement, consistent with the requirements of the Breach Notification Rule.[824]

Depending on the size of the regulated entity, the number of security incidents it experiences may vary, ranging from the occasional incident experienced by a small regulated entity to more than 1,000 per hour for a large regulated entity.[825] Given that such incidents may have little to no effect if the regulated entity's electronic information systems are able to deter it, it may not be necessary for a business associate to report the security incidents immediately to a covered entity (or a subcontractor to a business associate).

Additionally, as discussed above, regulated entities are required to establish, and implement as needed, a contingency plan[826] that includes the policies and procedures for responding to an emergency or other occurrence that damages systems that contain ePHI. Such emergencies or other occurrences could include a fire, vandalism, system failure, or a natural disaster.[827] The Department believes that, in some instances, a security incident would also be an emergency or other occurrence that could require a regulated entity to activate its contingency plan.[828] As the Department previously explained, a contingency plan is the only way to protect the confidentiality, integrity, and availability of ePHI during unexpected events that may expose ePHI because the usual security measures may be disabled, ignored, or not observed.[829]

b. Issues To Address

In recent years, there has been an increase in the number and types of emergencies or other occurrences that cause damage to systems that contain ePHI and may require a regulated entity to activate its contingency plan. For example, we have experienced an increase in extreme weather events over the last 40 years as a result of the changing climate.[830] Additionally, as discussed in greater detail above, there has been a significant increase in the number of breaches of unsecured PHI reported to the Department over the last five years.[831] And increasingly, ePHI is created, received, maintained, and transmitted using cloud-based software that may be located in a remote location, which means that covered entities more frequently rely on business associates to access ePHI.[832] Not only could the covered entity's ability to access ePHI or the relevant electronic information systems of the business associate that are affected by such an event, but the incident could also have repercussions for the covered entity's ePHI or its relevant electronic information systems. For example, a business associate's relevant electronic information systems may become infected with malicious software that spreads across devices connected to a network (*e.g.,* the NotPetya malware.[833]) If the covered entity is also connected to the same network, providing prompt notice to the covered entity of the security incident and activation of its contingency plan could enable the covered entity to prevent or mitigate damage to the covered entity's relevant electronic information systems.

When considered altogether, these developments mean that a regulated entity is more likely to experience an emergency or other occurrence that damages systems that contain ePHI than it was in either 2003[834] or 2013.[835] Unfortunately, based on the Department's experience, neither the increased risk nor the Security Rule's requirement that a business associate notify a covered entity (or that a subcontractor notify a business associate) of any security incident, including breaches of unsecured PHI, has been sufficient to encourage prompt notifications by a business associate to the covered entity (or of a subcontractor to a business associate) that its ability to

[821] Section 164.504(e) provides that when a covered entity and its business associate are both governmental entities, they do not have to negotiate a business associate agreement and may provide adequate assurances for its uses and disclosures of PHI if they enter into a memorandum of understanding or adopt a regulation that has the force and effect of law that incorporates the requirements of a business associate agreement. 65 FR 82462, 82597, 82677 (Dec. 28, 2000); *see also* 68 FR 8334, 8360 (Feb. 20, 2003) (§ 164.314(a) provisions are drawn from and intended to support the analogous privacy protections provided for by 45 CFR 164.504(e) and discussed in the 2000 Privacy Rule.); 78 FR 5566, 5590 (Jan. 25, 2013) (removed the specific requirements under 45 CFR 164.314 for a memorandum of understanding when both a covered entity and business associate are government entities and referred to the parallel requirements of the Privacy Rule at 45 CFR 164.504(e)(3)).

[822] 45 CFR 164.304 (definition of ''Security incident'').

[823] *See* 45 CFR 164.314(a).

[824] Where a business associate experiences a security incident that meets the definition of a breach at 45 CFR 164.402, the business associate must comply with the requirements of the Breach Notification Rule. *See* 45 CFR part 160 and subparts A and D of 45 CFR part 164. Specifically, the Breach Notification Rule requires a business associate to report a breach of unsecured PHI to a covered entity without unreasonable delay and in no case later than 60 days from the discovery of the breach. *See* 45 CFR 164.410(b).

[825] Testimony of Andrew Witty, *supra* note 214 (According to CEO Andrew Witty, intruders attempt to gain access to UnitedHealth Group's electronic information systems every 70 seconds, or more than 450,000 times per year.).

[826] 45 CFR 164.308(a)(7)(i).

[827] *Id.*

[828] *See* 45 CFR 164.308(a)(7)(i); proposed 45 CFR 164.308(a)(13)(i).

[829] 68 FR 8334, 8351 (Feb. 20, 2003).

[830] ''Since 1980, the United States has experienced 265 weather and climate disasters in which the overall damages reached or exceeded US$1 billion.'' Kristie L. Ebi, et al., ''Extreme Weather and Climate Change: Population Health and Health System Implications,'' Annual Review of Public Health (Jan. 2021), *https://pubmed.ncbi.nlm.nih.gov/33406378/; see also* ''Climate Change Indicators: U.S. and Global Temperature,'' U.S. Environmental Protection Agency (June 27, 2024) (''2023 was the warmest year on record [. . .] and 2014–2023 was the warmest decade on record since thermometer-based observations began.''), *https://www.epa.gov/climate-indicators/climate-change-indicators-us-and-global-temperature.*

[831] ''Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance, For Calendar Year 2022,'' Office for Civil Rights, U.S. Department of Health and Human Services, p. 8 (2022) (From 2018 to 2022, the number of breaches affecting fewer than 500 individuals increased 1 percent and breaches affecting 500 or more individuals rose 107 percent.), *https://www.hhs.gov/sites/default/files/compliance-report-to-congress-2022.pdf.*

[832] ''Unraveling the role of cloud computing in health care system and biomedical sciences,'' *supra* note 632 (''These days numerous commercial merchants are intermingling with hospitals as well as healthcare providers to establish healthcare-based cloud computing networks.''); *see also id.* (''[. . .] Microsoft, Google and Amazon have instantly realized that the majority of hospitals will not continue working with servers that are privately owned as well as controlled.''); ''Increase in healthcare cyberattacks affecting patients with cancer,'' *supra* note 180 (In 2021, an attack against oncology services targeted data stored in cloud-based systems and affected patients in several States.).

[833] Nicole Perlroth, et al., ''Cyberattack Hits Ukraine Then Spreads Internationally,'' The New York Times (June 27, 2017) (discussing a worldwide ransomware attack in 2017), *https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html.*

[834] *See* 68 FR 8334 (Feb. 20, 2003).

[835] *See* 78 FR 5566 (Jan. 25, 2013).

access ePHI or the electronic information systems that create, receive, maintain, or transmit ePHI may be affected. This lack of prompt notification delays a covered entity (or business associate) from responding and protecting its ePHI and electronic information systems accordingly.

c. Proposal

To address these risk trends and deficiencies in protections, the Department proposes to add an implementation specification at proposed 45 CFR 164.314(a)(2)(i)(D) that would require a business associate agreement to include a provision for a business associate to report to the covered entity activation of its contingency plan that would be required under 45 CFR 164.308(a)(13) without unreasonable delay, but no later than 24 hours after activation.[836] This proposal, if finalized, would not alter the business associate's breach reporting obligations under the Breach Notification Rule.[837] The Department believes that it is necessary to notify the covered entity in a timely manner of the contingency plan activation because of the downstream implications for such activation. Receiving such prompt notice could enable the covered entity to take the necessary steps to protect its own relevant electronic information systems, as well as to implement its own contingency plan if necessary and appropriate (*e.g.,* enable the covered entity to access a remote or offline backup of its ePHI if necessary to ensure that patient care is unaffected—or to reduce the effect on patient care as much as possible). For example, in 2020, a software company was the target of an attack that used software containing malware to infiltrate the electronic information systems of subsequent users of the software. This allowed cybercriminals to gain access to several government systems and thousands of private systems worldwide.[838] Requiring a business associate to provide prompt notice to the covered entity when the business associate activates its contingency plan could enable regulated entities to maintain individuals' confidence in their commitment to protecting the confidentiality, integrity, and availability of ePHI in the event of an emergency or other occurrence that adversely affects relevant electronic information systems.[839] Additionally, the modified standard would align with the enhanced CPG for Third Party Incident Reporting because this proposal would require a business associate to both report to a covered entity or another business associate activation of its contingency plan within 24 hours of such activation and report known or suspected security incidents.[840]

As discussed above, the Department proposes to require a regulated entity to activate its contingency plan to respond to an emergency or other occurrence that adversely affects relevant electronic information systems.[841] The Department believes that regulated entities activate their contingency plans infrequently because such plans are only activated when there is an emergency or other occurrence that rises to a level beyond a security incident that is thwarted or other event that does not adversely affect the confidentiality, integrity, or availability of ePHI. Thus, the need to make the proposed notification would also arise infrequently.

For example, a business associate may not be required to notify a covered entity within a certain time after a relevant electronic information system receives a basic internet command such as a ping,[842] which happens frequently. This is because a ping in and of itself generally does not adversely affect relevant electronic information systems when it is blocked by firewall policies, and thus does not require activation of the regulated entity's contingency plan. Instead, the business associate would be required to provide such notice in instances where internet commands received by the business associate indicate potential malicious activity, such as a denial of service attack, leading to activation of its contingency plan because of an event that adversely affects the business associate's relevant electronic information systems that create, receive, maintain, or transmit ePHI or adversely affects the confidentiality, integrity, or availability of its ePHI. However, in both such instances, a business associate would still be required to provide notice to the covered entity of the ping as a security incident in accordance with the business associate agreement.[843]

The proposal itself would only require that the business associate notify the covered entity of its activation of the contingency plan; it does not include any specific requirements with respect to the form, content, or manner of the notice. Instead, we propose to permit the covered entity and business associate to negotiate such terms and include them in their business associate agreement if they so choose.

We recognize that when such an emergency or other occurrence transpires, the focus of the affected regulated entity must be on activating its contingency plan and restoring access to ePHI and the affected relevant electronic information systems. Similarly, when the contingency plan activation is in response to a successful security incident,[844] it may take some time to investigate and determine the cause of the security incident. Thus, this proposal would not require reporting on the cause of the contingency plan activation; it would require reporting solely on the fact that it has activated the plan. Accordingly, we believe that 24 hours would provide a business associate with sufficient time to do all of the following: determine that there is an emergency or other occurrence adversely affecting the business associate's relevant electronic information systems; determine that it needs to activate its contingency plan; identify any covered entities that need to be notified; and notify such covered entities.

This proposed requirement to provide notice without unreasonable delay, but no later than 24 hours after a

[836] A subcontractor of a business associate also would be required to make such report to the business associate. *See* 45 CFR 164.314(a)(2)(iii) (applying the requirements in paragraphs (a)(2)(i) and (ii) to business associate agreements between business associates and subcontractors in the same manner as they apply to business associate agreements between covered entities and business associates).

[837] *See* 45 CFR 164.410.

[838] Saheed Oladimeji, et al., ''SolarWinds hack explained: Everything you need to know,'' TechTarget (Nov. 3, 2023) (SolarWinds is a software company and one of its products that was part of a supply chain attack is an IT performance monitoring system that had privileged access to IT systems.), *https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.*

[839] As discussed in greater detail above, the Department is proposing to renumber the standard for the contingency plan as 45 CFR 164.308(a)(13) and to require a written contingency plan for responding to an emergency or other occurrence that adversely affects relevant electronic information systems, as opposed to the current standard which applies when the emergency or other occurrence damages information systems that contain ePHI.

[840] Proposed 45 CFR 164.314(a)(2)(i)(C) and (D); ''Cybersecurity Performance Goals,'' *supra* note 18.

[841] Proposed 45 CFR 164.308(a)(13)(i).

[842] The ping command is a network diagnostic, and firewalls often block incoming pings to prevent attackers from learning more about the organization's network. Karen Scarfone, et al., ''Guidelines on Firewalls and Firewall Policy,'' NIST Special Publication 800–41, Revision 1, National Institute of Standards and Technology, U.S. Department of Commerce, p. 31 (Sept. 2009), *https://doi.org/10.6028/NIST.SP.800-41r1.*

[843] 45 CFR 164.314(a)(2)(i)(C).

[844] While we are proposing in this NPRM in 45 CFR 164.308(a)(13)(i) to specifically include a security incident as an example of an emergency or occurrence that may damage a relevant electronic information system for which a contingency plan would be required, we believe that this is a clarification, rather than a change.

contingency plan is activated, would also apply when a business associate that is a governmental entity enters into an arrangement with a covered entity that is also a governmental entity where such arrangement meets the requirements of the Privacy Rule at 45 CFR 164.504(e)(3) in accordance with 45 CFR 164.314(a)(2)(ii) and when a business associate enters into a business associate agreement with a subcontractor in accordance with 45 CFR 164.314(a)(2)(iii) to notify its business associate when it has activated its contingency plan.

Additionally, the Department proposes conforming changes to the references of 45 CFR 164.308(b) throughout 45 CFR 164.314 consistent with proposals made to modify 45 CFR 164.308(b). The Department does not intend these to be substantive changes, but rather an alignment with the proposed structural modifications in 45 CFR 164.308(b).

As discussed above, the Department proposes to remove the term ''required'' from the implementation specification at 45 CFR 164.314(a)(2) consistent with its proposal to eliminate the distinction between addressable and required implementation specifications. We also propose a few miscellaneous non-substantive corrections to update citations in the standard at 45 CFR 164.314(a)(1)(i) and (a)(2)(iii). We do not believe that these technical amendments would add or change any regulatory, recordkeeping, or reporting requirements, nor would they change the Department's interpretation of any regulation.

2. Section 164.314(b)(1)—Standard: Requirements for Group Health Plans

a. Current Provision

The second standard in 45 CFR 164.314 requires that, except when ePHI disclosed to a plan sponsor is summary health information [845] or enrollment or disenrollment information,[846] group health plan [847] documents must provide that the plan sponsor will reasonably and appropriately safeguard ePHI created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. Section 164.314(b)(2) requires that the plan documents of a group health plan must be amended to incorporate provisions to require the plan sponsor to:

- Implement reasonable and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan.[848]
- Ensure that the separation between the group health plan and plan sponsor required by the Privacy Rule at 45 CFR 164.504(f)(2)(iii) [849] is supported by reasonable and appropriate security measures.[850]
- Ensure that any agent to whom it provides ePHI, agrees to implement reasonable and appropriate security measures to protect the information.[851]
- Report to the group health plan any security incident of which it becomes aware.[852]

b. Issues To Address

Plan sponsors are not directly liable for compliance with the Security Rule because they are not regulated entities, *i.e.,* covered entities or business associates under HIPAA. Therefore, plan sponsors' obligations to apply safeguards to ensure the confidentiality, integrity, and availability of ePHI are limited to the requirements set forth in the plan documents of its group health plan. While 45 CFR 164.314(b) generally requires that plan documents call for the implementation of Security Rule-like safeguards, the current provision does not specifically require the group health plan to require the plan sponsor or any agent to whom it provides ePHI to comply with the requirements of the Security Rule. Given the concerns we have regarding Security Rule compliance generally by regulated entities, the Department is also concerned that group health plans have not sufficiently ensured that plan documents require that plan sponsors reasonably and appropriately safeguard ePHI created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. Additionally, the Department is concerned that group health plans may not be monitoring plan sponsors to ensure that ePHI is disclosed to a plan sponsor only if the plan sponsor voluntarily agrees to use and disclose the information only as permitted or required by the regulations.[853]

Plan sponsors may perform certain functions that are integrally related to, or similar to, the administrative functions of group health plans, and in carrying out these functions, need access to ePHI held by the group health plan. For example, plan sponsors may perform plan administration functions on behalf of the group health plan which are specified in plan documents. The increase in cybercrime and other emergencies adversely affecting electronic information systems is not limited to regulated entities or to the health care sector; plan sponsors are experiencing similar increases in events that require the activation of contingency plans.[854] And plan sponsors may not be reasonably and appropriately protecting the confidentiality, integrity, and availability of ePHI absent an express requirement that plan documents obligate a plan sponsor to implement the security measures in the Security Rule. Additionally, regulated entities may not have the ability to determine whether alternate security measures will accomplish the same result because they do not have access to the information systems of plan sponsors, nor would it be appropriate for them to have such access.

Additionally, the Department believes that prompt notification by a plan sponsor to the group health plan that the ability of the plan sponsor or the group health plan to access ePHI or relevant electronic information systems may be affected by a security incident is important for the same reasons discussed above in 45 CFR 164.314(a). This lack of prompt notification delays a group health plan from responding and protecting its ePHI and relevant electronic information systems accordingly.

c. Proposal

The Department proposes to modify the implementation specifications at 45 CFR 164.314(b)(2)(i) through (iii) to address concerns that group health plans may not recognize that reasonable and appropriate safeguarding of ePHI requires the implementation of security measures that are the same as, or at least equivalent to, the security measures in the Security Rule. First, we propose to rename the implementation specifications as ''Safeguard implementation,'' ''Separation,'' and

[845] *See* 45 CFR 164.504(f)(1)(ii).

[846] *See* 45 CFR 164.504(f)(1)(iii).

[847] 45 CFR 160.103 (definition of ''Group health plan'').

[848] 45 CFR 164.314(b)(2)(i).

[849] 45 CFR 164.504(f)(2)(iii) requires the plan documents to describe an employee or class of employee who receives PHI for payment, health care operations or other matters related to the group health plan; restrict access to PHI and use of PHI by such employees to the plan administration functions that the plan sponsor performs for the group health plan; and provide an effective mechanism for resolving any issues of noncompliance by such persons.

[850] 45 CFR 164.314(b)(2)(ii).

[851] 45 CFR 164.314(b)(2)(iii).

[852] 45 CFR 164.314(b)(2)(iv).

[853] 65 FR 82462, 82508 (Dec. 28, 2000).

[854] *See* ''2024 Data Breach Investigations Report,'' Verizon Business (2024), *https://www.verizon.com/business/resources/reports/dbir/.*

''Agents,'' respectively. We also propose to modify all three implementation specifications to require that plan documents of the group health plan would obligate a plan sponsor or any agent to whom it provides ePHI to implement the administrative, physical, and technical safeguards of the Security Rule. The Department recognizes that plan sponsors may need access to ePHI in certain situations, such as when they perform functions that are integrally related to, or similar to, those performed by group health plans, and we believe that such information must be protected by plan sponsors in the same manner in which it is protected by group health plans and other regulated entities.[855]

The security measures we are proposing in this NPRM are consistent with the CISA Cross-Sector CPGs,[856] and thus should be consistent with measures plan sponsors are implementing to protect their own electronic information systems, regardless of the obligations imposed on them by plan documents. For example, the Department seeks to ensure that plan sponsors are implementing administrative safeguards, such as performing a risk analysis,[857] to protect the confidentiality, integrity, and availability of all ePHI in its information systems; documenting required policies and procedures; and documenting implementation of such administrative safeguards, including the required policies and procedures.[858] Thus, requiring plan sponsors to implement the same security measures that regulated entities are implementing would maintain confidence in the commitment of plan sponsors to protecting the confidentiality, integrity, and availability of ePHI in light of the increasing cybersecurity threats as discussed above.

Additionally, the Department proposes to rename the implementation specification at 45 CFR 164.314(b)(2)(iv) as ''Security incident awareness.''

Similar to the discussion above, the Department proposes to add a new implementation specification for contingency plan activation at proposed 45 CFR 164.314(b)(2)(v) that would require plan documents to include a provision requiring a plan sponsor to report to the group health plan without unreasonable delay, but no later than 24 hours after activation of its contingency plan.[859] As discussed above, the Department believes that a group health plan needs to be notified in a timely manner when a plan sponsor activates its contingency plan because of the potential implications on the ability of a group health plan to protect the confidentiality, integrity, and availability of ePHI in its relevant electronic information systems. Accordingly, we believe that 24 hours would provide a plan sponsor sufficient time to do all of the following: determine that there is an emergency or other occurrence adversely affecting the plan sponsor's relevant electronic information systems; determine that it needs to activate its contingency plan; activate its contingency plan; identify any group health plans that need to be notified; and notify such group health plans.

Similarly, as discussed above, we propose to permit the group health plan and plan sponsor to negotiate the form, content, or manner of the notice and include them in their plan documents if they so choose.

The Department believes that requiring a plan sponsor to provide prompt notice to the group health plan when the plan sponsor activates its contingency plan would enable group health plans and plan sponsors to maintain individuals' confidence in their commitment to protecting the confidentiality, integrity, and availability of ePHI.

Additionally, consistent with our proposal to revise 45 CFR 164.306, the Department proposes to remove the term ''required'' from the implementation specification at 45 CFR 164.314(b)(2) consistent with our overall proposal to eliminate the distinction between ''required'' and ''addressable'' implementation specifications. However, a regulated entity would still be required to comply with all standards and implementation specifications as applicable to its situation, as proposed in 45 CFR 164.306(c).

3. Request for Comment

The Department requests comment on the foregoing proposals, including any benefits, drawbacks, or unintended consequences. We also request comment on the following considerations in particular:

a. How group health plans currently ensure that plan sponsors implement reasonable and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of ePHI.

b. Whether it is appropriate for group health plans to require plan sponsors to implement the administrative, physical, and technical safeguards of the Security Rule. If not, please explain and provide alternatives for how the Department should ensure the confidentiality, integrity, and availability of ePHI when it is disclosed to plan sponsors.

c. Whether business associates currently notify covered entities (or subcontractors notify business associates) upon activation of their contingency plans, and if so, the manner and timing of such notice.

d. Whether plan sponsors currently notify group health plans upon activation of their contingency plans, and if so, the manner and timing of such notice.

e. Whether it would be appropriate to require a business associate to notify a covered entity (or a subcontractor to notify a business associate) within 24 hours of activating its contingency plan. If not, please explain why and what would be an appropriate amount of time for such notification.

f. Whether it would be appropriate to require a plan sponsor to notify a group health plan within 24 hours of activating its contingency plan. If not, please explain why and what would be an appropriate amount of time for such notification.

g. The manner, timing, frequency, and process used by business associates to report security incidents to a covered entity (or subcontractors to business associates).

h. The manner, timing, frequency, and process used by a plan sponsor to report security incidents to a group health plan.

H. Section 164.316—Documentation Requirements

1. Current Provisions

Section 164.316(a) requires a regulated entity to implement reasonable and appropriate policies and procedures that comply with the Security Rule, taking into account the size, complexity, and capabilities of the regulated entity;[860] the regulated entity's technical infrastructure, hardware, and software capabilities;[861] the costs of security measures;[862] and the probability and criticality of

[855] 65 FR 82462, 82508 (Dec. 28, 2000); *see also* 68 FR 8334, 8360 (Feb. 20, 2003) (§ 164.314(b) provisions are drawn from and intended to support the analogous privacy protections provided for by 45 CFR 164.504(f) and discussed in the 2000 Privacy Rule.).

[856] ''Cross-Sector Cybersecurity Performance Goals,'' *supra* note 164.

[857] Proposed 45 CFR 164.308(a)(2)(i).

[858] Proposed 45 CFR 164.308, 164.310, 164.312, and 164.316.

[859] The plan sponsor would implement a contingency plan because it is one of the requirements of the administrative safeguards of the Security Rule and would be implemented based on the proposed requirements in 45 CFR 164.314(b)(2)(i).

[860] 45 CFR 164.306(b)(2)(i).

[861] 45 CFR 164.306(b)(2)(ii).

[862] 45 CFR 164.306(b)(2)(iii).

potential risks to ePHI.[863] Such policies and procedures must be consistent with the other requirements of the Security Rule. A regulated entity is permitted to change its policies and procedures, but it must document and implement such change in accordance with the Security Rule.

The standard and implementation specifications for documentation are in 45 CFR 164.316(b). Paragraph (b)(1) requires a regulated entity to maintain the policies and procedures it implements to comply with the Security Rule in written form. Additionally, where the Security Rule requires an action, activity, or assessment to be documented, the regulated entity must maintain a written record of the action, activity, or assessment. In both cases, the written record may be electronic. Paragraph (b)(2) includes the current implementation specifications for the documentation standard. Such documentation must be retained for the later of either: (1) six years from its creation, or (2) the date it was last effective. Additionally, it must be available to those responsible for implementing the documented policies and procedures. Finally, regulated entities must periodically review their documentation and update it as needed in response to environmental or operational changes affecting the security of ePHI.

2. Issues To Address

Although this section currently addresses policies and procedures and documentation, it does not require or include standards to govern how regulated entities must implement, maintain, and document implementation of all security measures. Implementing, maintaining, and documenting implementation of all security measures is important to ensure that regulated entities make well-reasoned decisions about implementing the requirements of this rule. Just as the Department believes that it is necessary to consider expanding the definition of ''security measures'' to better reflect that security measures should be multi-layered, we also believe that it is necessary to consider providing a more complete instruction concerning how regulated entities must implement, maintain, and document their implementation of the required security measures.

Additionally, OCR's own experience in investigations and audits leads us to believe that many regulated entities may not be documenting their security measures or their implementation of those measures.[864] It is critical for a regulated entity to commit to writing the security measures required by the Security Rule to ensure consistent implementation and compliance with the Security Rule. Verbal instructions may be forgotten or misconstrued, and what the regulated entity believes to be common knowledge may not be or may be relayed incorrectly between workforce members.

Additionally, based on OCR's enforcement experience, the Department believes that regulated entities may not be periodically reviewing and updating their documentation when they modify their security measures in response to environmental or operational changes affecting the security of their ePHI. Given the constant evolution of technology and the everchanging behavior of cybercriminals in response to technological evolution, the Department believes that regular review of cybersecurity-related security measures is essential for protecting the confidentiality, integrity, and availability of ePHI and relevant electronic information systems.

3. Proposals

As discussed above, the Department has proposed to revise other provisions of the Security Rule to clarify the differences between administrative and technical safeguards and between policies and procedures on the one hand and technical controls on the other hand. We have also proposed to revise other provisions of the Security Rule to clarify that a regulated entity is required to implement and maintain its administrative, physical, and technical safeguards, including its policies and procedures. These proposals clarify that such maintenance requires the review, testing, and modification of the regulated entity's security measures on a regular cadence, meaning that the regulated entity's security measures can be modified at any time. Given these proposals, the Department believes that we must also propose to revise 45 CFR 164.316 to delete the standard for policies and procedures and to modify the Security Rule's documentation requirements. Accordingly, the Department proposes to rename this section as ''Documentation Requirements'' and to redesignate the documentation standard as paragraph (a). We also propose to require that a regulated entity document how it considered the factors in 45 CFR 164.306(b) in the development of its written policies and procedures.

We also propose to modify the documentation standard to clarify that all required written documentation may be in electronic form. Additionally, we propose to modify the standard's two paragraphs. Specifically, the Department proposes at proposed 45 CFR 164.316(a)(1) to require that a regulated entity document the policies and procedures it has implemented to comply with the Security Rule, and as part of that documentation, explain how it considered the factors at 45 CFR 164.306(b) in the development of its policies and procedures. Relatedly, we also propose to modify 45 CFR 164.316(a)(2) to require a regulated entity to document all of the actions, activities, and assessments required by the Security Rule. The Department believes that both proposals would help to address two common problems observed in Security Rule investigations: a failure by the regulated entity to document its policies and procedures and a failure to document actions, activities, and assessments taken to comply with the Security Rule. Without such documentation, it is challenging for a regulated entity to assess and ensure its own compliance. Accordingly, we believe that our proposals to require a regulated entity to document its implementation of the Security Rule requirements would aid both the regulated entity and the Department.

Consistent with our proposal to redesignate the documentation standard as 45 CFR 164.316(a), we propose to redesignate the implementation specifications for documentation time limits, availability, and updates as proposed at 45 CFR 164.316(b)(1) through (3), respectively. Under proposed 45 CFR 164.316(b)(3), the Department proposes to require a regulated entity to update its documentation at least once every 12 months and within a reasonable and appropriate period of time after a security measure is modified.[865] As

[863] 45 CFR 164.306(b)(2)(iv).

[864] *See* Resolution Agreement, ''Peachstate Health Management, Inc.,'' Office for Civil Rights, U.S. Department of Health and Human Services (Apr. 28, 2021), *https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/peachstate/index.html;* ''West Georgia Ambulance, Inc.,'' *supra* note 583; *see also* ''2016–2017 HIPAA Audits Industry Report,'' *supra* note 121, p. 27 (the Department found that only 31 percent of regulated entities audited had safeguarded ePHI through risk analysis activities, including developing and implementing policies and procedures).

[865] In 2003, the Department declined a commenter's suggestion to change the term ''periodically'' to ''at least annually.'' At that time, we said that documentation must be updated as needed to reflect security measures currently in effect and that the requirement allowed individual entities to establish review and update cycles as deemed necessary because it would vary dependent

Continued

discussed above, the Department recognizes that the health care environment has changed in a way that necessitates thorough and frequent review of and updates to documentation. By proposing to specify how often documentation must be updated, the Department would clarify that we expect regulated entities to review and update their documentation at regular intervals, in addition to doing so in response any changes to a security measure. Cybersecurity and data protection is an evolving process, which makes formal, updated, and detailed documentation imperative for data protection. By reviewing and updating its documentation, including its written policies and procedures, at least annually and in response to changes to its security measures, a regulated entity should have a full understanding of its implemented security measures and be able to determine which measures should be updated to protect the confidentiality, integrity, and availability of ePHI.

As discussed above and consistent with the proposed changes to 45 CFR 164.306, the Department is proposing to remove the term ''required'' from 45 CFR 164.316(b)(1) through (3).

4. Request for Comment

The Department requests comment on the foregoing proposals, including any benefits, drawbacks, or unintended consequences. We also request comment on the following consideration in particular:

a. Whether it would be appropriate to require regulated entities to review and update documentation for security measures at least once every 12 months. If not, please explain.

b. Whether it is clear that 45 CFR 164.316 provides regulated entities with directions on when and how they are to document all security measures across all safeguard requirements. If not, please explain.

c. Whether it is feasible for regulated entities to document all of the actions, activities, and assessments required by the Security Rule as proposed at 45 CFR 164.316(a)(2). If not, please explain.

I. Section 164.318—Transition Provisions

1. Current Provisions and Issues To Address

Section 164.318 established the compliance dates for the initial implementation of the security standards for health plans, health care clearinghouses, and health care providers in 2005 and 2006.[866] Covered entities have been required to comply with the security standards for almost 20 years, and the initial implementation of the security standards is no longer applicable. Because of this, the Department believes that these provisions are no longer necessary.

2. Proposal

The Department proposes to remove the information in 45 CFR 164.318 and replace the language with provisions for transitioning to the revised Security Rule, should the proposals included in this NPRM be adopted.

The Department understands that regulated entities may be concerned with the anticipated administrative burden and cost of revising their business associate agreements or other written arrangements to comply with a revised Security Rule. For example, a regulated entity would need to update its business associate agreements to add a provision specifying that the business associate will report to the covered entity[867] that it activated its contingency plan no later than 24 hours after activation of such plan.[868] A regulated entity may have existing contracts that are not set to terminate or expire until after the compliance date for a final rule modifying the Security Rule, and we understand that a six-month compliance period may not provide enough time to reopen and renegotiate all contracts, in addition to ensuring that all regulated entities are compliant with the revised Security Rule. Accordingly, the Department proposes to relieve some of the burden on regulated entities by adding a specified period of transition for certain existing contracts.

The Department's authority to provide a transition period is expressed in 45 CFR 160.104(c), which allows the Secretary to establish the compliance date for any modified standard or implementation specification, considering the extent of the modification and the time needed to comply with the modification.[869]

Given these considerations, to allow regulated entities enough time to update thousands of existing business associate agreements or other written arrangements, the Department proposes to provide additional time to update the contracts required by 45 CFR 164.314(a)(1).

Specifically, the Department proposes to add new transition provisions under 45 CFR 164.318 to allow regulated entities to continue to operate under certain existing business associate agreements or other written arrangements until the earlier of: (1) the date such contract or other arrangement either is renewed on or after the compliance date of the final rule; or (2) a year after the effective date of the final rule. The additional transition period would be available to regulated entities if both of the following conditions are met: (1) prior to the publication date of the final rule, the covered entity or business associate had an existing business associate agreement or other written arrangement with a business associate or subcontractor, respectively, that complied with the Security Rule prior to the effective date of a final rule revising the Security Rule; and (2) such contract or arrangement would not be renewed or modified between the effective date and the compliance date of the final rule.

Under the proposed transition provisions, a business associate would be permitted to create, receive, maintain, or transmit ePHI pursuant to an existing business associate agreement or other written arrangement with another regulated entity that does not require the regulated entity to obtain satisfactory assurances that meet the requirements of the revised Security Rule for up to one year after the revised Security Rule becomes effective, assuming that a final Security Rule is published; and that the agreement is compliant with the Security Rule at the time the final rule is published and that it is not renewed or modified between the effective and compliance dates.[870] The transition provisions would also allow for the business associate to create, receive, maintain, or transmit ePHI on behalf of another regulated entity where the existing business associate agreement does not require that the regulated entity verify that the

upon a given entity's size, configuration, environment, operational changes, and the security measures implemented. 68 FR 8334, 8361 (Feb. 20, 2003).

[866] HIPAA set forth the compliance dates for the initial standards. 42 U.S.C. 1320d–4; *see also* 68 FR 8334, 8351 (Feb. 20, 2003).

[867] Similarly, a business associate subcontractor would need to report to the business associate. *See* ''Business Associate Contracts,'' Office for Civil Rights, U.S. Department of Health and Human Services (June 16, 2017) (A ''business associate'' also is a subcontractor that creates, receives, maintains, or transmits PHI on behalf of another business associate), *https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.*

[868] Proposed 45 CFR 164.314(a)(2)(i)(D).

[869] The Department has previously included transition provisions to ensure that important functions of the health care system were not impeded. *See, e.g.,* 65 FR 82462 (Dec. 28, 2000); 67 FR 53182 (Aug. 14, 2002); 78 FR 5566 (Jan. 25, 2013).

[870] *See* proposed 45 CFR 164.308(b)(1)(i).

business associate has deployed technical safeguards in accordance with the Security Rule under the same circumstances as those described above.[871]

During the transition period, the Department proposes to allow a business associate to create, receive, maintain, or transmit ePHI pursuant to a business associate agreement or other written arrangement with another regulated entity without including in the agreement that the business associate will: (1) comply with the revised Security Rule;[872] (2) ensure that any subcontractors that create, receive, maintain, or transmit ePHI on behalf of the business associate agree to comply with the revised Security Rule by entering into a business associate agreement or other arrangement that meets the requirements of the revised rule;[873] and (3) report to the covered entity[874] activation of its contingency plan.[875]

Additionally, the Department intends that, in cases where a contract renews automatically without any change in terms or other action by the parties (also known as ''evergreen contracts''), such contracts would be eligible for the extension if they automatically renew between the effective and compliance dates. Thus, regulated entities with an evergreen contract will be deemed to be in compliance with the Security Rule's requirements for business associate agreements or other written arrangements and such deemed compliance would not terminate when these contracts automatically renew. These transition provisions would apply to written contracts or other written arrangements as specified above.

These transition provisions would apply only to the requirement to amend contracts or other arrangements with business associates, and they would not affect any other compliance obligations under the Security Rule. For example, beginning on the compliance date of the final rule, assuming a final rule is published and that it is finalized as proposed, a business associate would be required to implement and document its implementation of the administrative, physical, and technical safeguards required by a revised Security Rule, except with respect to 45 CFR 164.308(b) and 164.314(a), even if the business associate's contract with the covered entity[876] has not yet been amended.

Given the possibility of a similar burden on group health plans and plan sponsors to update plan documents by the compliance date, the Department is considering, but not proposing, a similar transition provision for plan documents. We are not proposing such provisions at this time because, unlike business associates, plan sponsors do not have independent obligations under the Security Rule. Instead, the obligations of plan sponsors are based entirely on the content of the plan documents. Accordingly, if the plan documents are not updated, plan sponsors are not obligated to comply with the requirements of the Security Rule because they are not regulated entities.

In particular, the Department is considering, but not proposing at this time, adding a new paragraph (d) introductory text under 45 CFR 164.318, with the heading ''Standard: Effect of prior plan documents for group health plans,'' stating that notwithstanding any other provisions of the subpart, a group health plan may allow a plan sponsor to create, receive, maintain, or transmit electronic protected health information pursuant to a written plan document with such group health plan that does not comply with § 164.314(b), only in accordance with paragraph (d)(1). The Department is also considering adding a new paragraph (d)(1) under 45 CFR 164.318, with the heading ''Implementation specification: Plan documents for group health plans,'' stating that the requirements of paragraph (b) apply to the plan document between a group health plan and a plan sponsor in the same manner as such requirements apply to written contracts or other arrangements between a covered entity and a business associate.

Similarly, the Department is considering, but not proposing at this time, adding a new paragraph (d)(2) under 45 CFR 164.318, with the heading ''Group health plan responsibilities,'' stating that nothing in the section shall alter the requirements of a group health plan or plan sponsor to comply with the applicable provisions of the part other than § 164.314(b).

3. Request for Comment

The Department requests comment on the foregoing proposals, including any benefits, drawbacks, or unintended consequences. We also request comment on the following considerations in particular:

a. Whether the Department's proposal to provide regulated entities with additional time to revise business associate agreements or other written contracts is appropriate. If not, please explain.

b. Whether the Department should also provide group health plans and plan sponsors additional time to revise plan documents by adding a transition provision to grandfather certain existing plan documents for a specified period of time.

c. Whether the Department should consider additional constraints or specificity for a new paragraph (d) to allow group health plans more time to comply with the Security Rule requirements for plan documents.

J. Section 164.320—Severability

The Department intends that, if any provisions of this subpart, including the provisions of this NPRM, if finalized, were held to be invalid or unenforceable facially, or as applied to any person, plaintiff, or stayed pending further judicial or agency action, such provision shall be severable from other provisions of this subpart, and from other rules and regulations currently in effect, and not affect the remainder of this subpart. It is also our intent that, unless such provision shall be held to be utterly invalid or unenforceable, it shall be construed to give the provision maximum effect to the provision permitted by law, including in the application of the provision to other persons not similarly situated or to other dissimilar circumstances from those where the provision may be held to be invalid or unenforceable.

The provisions of this subpart, including the proposals of this NPRM, are intended to operate independently of each other, even if multiple provisions serve the same or similar general purpose(s) or policy goal(s). Where a provision is necessarily dependent on another, the context generally makes that clear, such as by cross-reference to a particular standard, requirement, or implementation specification. Where a provision that is dependent on one that is stayed or held invalid or unenforceable, as described in the preceding paragraph, is included in paragraph or section within 45 CFR part 160 or 164, we intend that other provisions of such paragraph(s) or section(s) that operate independently of said provision would remain in effect.

The Department intends the individual standards in 45 CFR 164.308, 164.310, 164.312, 164.314, and 164.316 to apply separately to govern how a regulated entity must protect the security of all ePHI it creates, receives,

[871] *See id.*

[872] 45 CFR 164.314(a)(2)(i)(A).

[873] 45 CFR 164.314(a)(2)(i)(B).

[874] Or to the business associate from a business associate subcontractor.

[875] Proposed 45 CFR 164.314(a)(2)(i)(D).

[876] Or business associate's contract with the subcontractor.

maintains, or transmits. Accordingly, if finalized, this provision would provide that if any one or several standards in 45 CFR 164.308, 164.310, 164.312, 164.314, and 164.316 are deemed invalid by a court, or non-applicable to a particular person or circumstance, all remaining standards shall be unaffected and shall remain in force, and any remaining component of the adjudicated provision, not invalid or found to be unenforceable or inapplicable, shall be considered by the Department to be still in effect.

For example, the standard for risk analysis proposed in 45 CFR 164.308(a)(2) would protect ePHI from risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI, while the modified standard for workforce security proposed in 45 CFR 164.308(a)(9) would protect ePHI from inappropriate access by a regulated entity's workforce. An invalidated standard for workforce security would not render the entire rule unworkable because a regulated entity could still meet the requirement to conduct the risk analysis without regard to whether the entity meets the requirements included in the standard for workforce security. Similarly, were a court to invalidate the Department's proposal in 45 CFR 164.310(a)(1) requiring that implemented policies and procedures to limit physical access to relevant electronic information systems and the facility or facilities in which they are housed be in writing, a regulated entity could still meet a requirement to implement the policies and procedures. Similar considerations apply to the proposal for written policies and procedures in proposed 45 CFR 164.316(a), and to proposals that are deemed inapplicable to certain persons or circumstances.

Further, the Department believes it is necessary to clarify how regulated entities would continue to apply implementation specifications in the event a court invalidates or deems inapplicable a governing standard over a specific implementation specification, or if a court invalidates or deems inapplicable one or several implementation specifications without taking adverse action on the governing standard. The Department does not interpret that this severability proposal, if finalized, would apply to implementation specifications in the same manner as it would apply to standards. Because the implementation specifications are regulatory instructions on how a regulated entity is to comply with a particular standard, if any standard is stricken, all implementation specifications underneath are similarly stricken. Conversely, the Department does not intend for the overarching standard to be affected by a court's decision to invalidate or make a determination of non-applicability to particular person or circumstance all implementation specifications under a particular standard. The Security Rule would still retain its flexible and scalable approach, and, therefore, a regulated entity could use any reasonable and appropriate security measure to implement the standard consistent with 45 CFR 164.306(b), even if all implementation specifications under the standard are stricken.

If a court invalidates or deems inapplicable less than all implementation specifications under a specific standard (*i.e.,* only one or several), the ability of a regulated entity to execute the remaining implementation specification(s) depends on whether the remaining implementation specifications are dependent on one another or operate together to impose requirements on regulated entities. For example, several proposed implementation specifications under the standard for facility access controls at 45 CFR 164.310(a)(1) would require a regulated entity to both establish and implement written procedures pertaining to specific requirements such as contingency operations, facility security planning and access control and validation, and then subsequently review the written policies and procedures every 12 months. Should a court invalidate or deem inapplicable the implementation specification to establish and implement written policies procedures, the secondary specification requiring review of said procedures would also become invalid.

The Department believes that each definition is independent of all other definitions.

This list of examples is not intended to be exhaustive. The absence from this list of any particular provision should not be construed to mean that the Department considers that provision to be not severable from other parts of the rule.

To ensure that our intent for severability of provisions is clear in the CFR, the Department proposes to add a section on severability at 45 CFR 164.320. Proposed 45 CFR 164.320 would state our intent that if any provision of this subpart is held to be invalid or unenforceable, it shall be construed to give maximum effect to the provision permitted by law unless the holding shall be one of utter invalidity or unenforceability, in which case the provision shall be severable from this subpart and shall not affect the remainder thereof or the application of the provision to other persons not similarly situated or to other dissimilar circumstances.

The Department requests comment on the foregoing proposal, including any benefits, drawbacks, or unintended consequences.

K. New and Emerging Technologies Request for Information

Technology is constantly evolving, able to perform increasingly complex tasks, including those with the potential to improve health care and communication between individuals and care providers. These new and evolved technologies will continue to transform health care in a variety of ways, including providing regulated entities with new tools for faster and more accurate diagnoses, effective treatments, and more efficient administration.

As a regulated entity considers the application of new technologies or the use of existing tools in innovative ways, it also must consider whether these technologies create, receive, maintain, or transmit ePHI, and, if so, how to secure them. The Security Rule was designed to be technology-neutral for this very reason and continues to provide the foundation for ensuring the confidentiality, integrity, and availability of all ePHI as technology changes.[877] As a result, while the technology may be new or developing, securing ePHI involved with the technology can be successfully executed through compliance with the Security Rule.

Before implementing new and emerging technologies, a regulated entity must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.[878] It must then implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.[879] Such administrative, physical, and technical safeguards apply to all instances of ePHI maintained or transmitted by the regulated entity, regardless of the technology used. Below, we discuss some examples of new technologies, such as quantum computing, AI, and virtual and augmented reality (VR and AR), and

[877] 45 CFR 164.306(a).

[878] 45 CFR 164.508(a)(1)(ii)(A).

[879] 45 CFR 164.308(a)(1)(ii)(B).

how the Security Rule would apply in each case.

1. Quantum Computing

Several Federal agencies have considered the potential benefits and drawbacks of quantum information science,[880] that is, the study of ''the impacts of quantum physics properties on information science. Those properties can increase computational power and speed significantly over classical computers, provide precision measurements; enhance sensing capabilities; and increase the accuracy of position, navigation, and timing services.'' [881] According to NIST, ''In recent years, there has been a substantial amount of research on quantum computers—machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers.'' [882]

However, the increase in computational capability threatens the security of asymmetric cryptography,[883] which is critical to encryption solutions, a key protection for ePHI and other sensitive information today. Scientists warn that when such quantum computers are built, they will have the ability to break many of the systems for asymmetric cryptography that are in use today.[884] Thus, experts anticipate that quantum computing will adversely affect the confidentiality and integrity of digital communications.[885] ''The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks.'' [886] A recent National Security Memorandum affirmed that ''alongside its potential benefits, quantum computing also poses significant risks to the economic and national security of the United States. . . . [including the potential to break] much of the public-key cryptography used on digital systems across the United States and around the world.'' [887] Accordingly, the White House has directed Federal agencies to take specific steps to ''mitigate the threat of [cryptanalytically relevant quantum computers] through a timely and equitable transition of the Nation's cryptographic systems to interoperable quantum-resistant cryptography.'' [888]

NCVHS examined these security issues and provided recommendations to the Department for applying the safeguards of the HIPAA Rules to potential quantum computing threats. Specifically, NCVHS declared that incorporation of recent Administration guidance for Federal agencies ''on vulnerable cryptographic systems is necessary to strengthen the Technical Safeguards within the Security Rule.'' [889] This joint guidance, developed by NIST, CISA, and NSA, encourages ''the early planning for migration to post-quantum cryptographic standards by developing a Quantum-Readiness Road map.'' [890] It also recommends that organizations prepare a cryptographic inventory, discuss post-quantum roadmaps with technology vendors, consider their supply chain's readiness for quantum computing, and consider the responsibilities of their technology vendors with respect to preparing for quantum readiness.[891]

The Department encourages regulated entities to incorporate these activities as part of their ongoing risk management programs. For example, the steps presented in the joint guidance—surveying the environment for potential risks and vulnerabilities that endanger ePHI, identifying workforce members with responsibility for addressing them, inventorying quantum-vulnerable systems, including that inventory in its risk analysis and risk management, and working with technology vendors to ensure their readiness—are all activities that already are required by the administrative safeguards of the Security Rule.

We believe these obligations would be clarified by the proposals in this NPRM. For example, the Department proposes to require that a regulated entity not only conduct an accurate assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of the ePHI it creates, receives, maintains, or transmits, but would add an express requirement that the assessment be comprehensive and in writing. We also propose to specify that the required assessment include, among other things, identification of all reasonably anticipated threats and potential vulnerabilities and predisposing conditions, making a reasonable determination and documentation of the likelihood that each identified threat will exploit the identified vulnerabilities, and performing a written assessment of the risk level for each identified threat and vulnerability. Under the NPRM, a regulated entity would be expected to, as part of the risk analysis, consider whether quantum computing poses a reasonably anticipated threat to the confidentiality, integrity, or availability of its ePHI and whether there is a vulnerability or predisposing condition that corresponds to that threat, and to document those considerations; make a reasonable determination and document the likelihood that the threat will exploit the identified vulnerabilities; and assign a risk level to the identified threat and vulnerability.

2. Artificial Intelligence (AI)

Section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 defined AI to include the following: [892]

- Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
- An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception,

[880] *See* ''Post-Quantum Cryptography, Quantum Background,'' U.S. Department of Homeland Security (last accessed July 23, 2024), *https://www.dhs.gov/quantum; see also* ''Quantum-Readiness: Migration to Post-Quantum Cryptography,'' Cybersecurity & Infrastructure Security Agency, National Security Agency, and National Institute of Standards and Technology, p. 1 (Aug. 21, 2023), *https://media.defense.gov/2023/Aug/21/2003284212/-1/-1/0/CSI-QUANTUM-READINESS.PDF.*

[881] ''Post-Quantum Cryptography, Quantum Background,'' *supra* note 880.

[882] *See* ''Post-Quantum Cryptography PQC,'' Computer Security Resource Center, National Institute of Standards and Technology, U.S. Department of Commerce (July 19, 2024), *https://www.nist.gov/pqcrypto.*

[883] *See* ''Post-Quantum Cryptography, Quantum Background,'' *supra* note 880.

[884] *See* ''Post-Quantum Cryptography PQC,'' *supra* note 882.

[885] *Id.*

[886] *See id.* (removed emphasis from ''post-quantum cryptography'' in original).

[887] National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, National Security Memorandum/NSM–10, The White House (May 4, 2022), *https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.*

[888] *Id.*

[889] *See* Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 2 (providing NCVHS recommendations to strengthen the HIPAA Security Rule).

[890] *See* ''Quantum-Readiness: Migration to Post-Quantum Cryptography,'' Cybersecurity & Infrastructure Security Agency, National Security Agency, and National Institute of Standards and Technology, p. 1 (Aug. 21, 2023), *https://media.defense.gov/2023/Aug/21/2003284212/-1/-1/0/CSI-QUANTUM-READINESS.PDF.*

[891] *Id.*

[892] Sec. 238(g) of Public Law 115–232, 132 Stat. 1697–98 (Aug. 13, 2018) (10 U.S.C. 2358 note) (definition of ''AI'').

cognition, planning, learning, communication, or physical action.

- An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
- A set of techniques, including machine learning, that is designed to approximate a cognitive task.
- An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

AI requires enormous amounts of data to develop, but it also has enormous potential benefits. The Department has previously stated that these ''technologies have the potential to drive innovation, increase market competition, and vastly improve care for patients and populations.'' [893] According to experts, ''[. . .]AI is unlocking new possibilities by advancing medicine in entirely unimaginable ways and solving some of the grand global healthcare challenges.'' [894] And FDA agrees: ''AI technologies are transforming health care by producing diagnostic, therapeutic, and prognostic medical recommendations, or decisions, in some cases independently, informed by the vast amount of data generated during the delivery of health care.'' [895] In medical devices, areas for AI application include:

- Image acquisition and processing
- Early disease detection
- More accurate diagnosis, prognosis, and risk assessment
- Identification of new patterns in human physiology and disease progression
- Development of personalized diagnostics
- Therapeutic treatment response monitoring [896]

For example, clinicians are using AI to distill large volumes of EHR information about a complex patient into a summarized note that they can use to consider diagnoses and treatment. AI also has been used for aid in the detection of diabetic retinopathy, screening for breast and lung cancer, and classification of skin conditions.[897] Others are using ambient AI scribes, a technology that uses microphones to transcribe encounters with patients in real-time.[898] This tool creates clinical documentation that clinicians can later edit, which can lead to improved interactions with patients and reduced time on documentation.[899] Newer AI tools may search medical records for relevant information regarding common conditions and other risk factors [900] or offer relevant questions for clinicians to pose to make an accurate diagnosis.[901]

Unfortunately, AI can also be used to harm individuals, both intentionally and unintentionally. Bad actors are using generative AI to threaten the privacy and security of ePHI more effectively through phishing and other social engineering. As explained by NCVHS, ''AI tools can create mass scale [cyberattacks] that are highly effective and major threats to ePHI.'' [902] Experts anticipate that AI ''will ultimately pioneer the malicious use of [. . .] 'Offensive AI'—highly sophisticated and malicious attack code—[that] will be able to mutate itself as it learns about its environment, and to expertly compromise systems with minimal chance of detection.'' [903] Such experts are concerned about the level of destruction that will lie in its wake and compare it to an arms race that can only escalate.[904] Indeed, it seems likely that regulated entities will need to invest in AI to defend against malicious use of AI in the future.[905]

After assessing current and potential AI threats, NCVHS recommended that the Department clarify how the HIPAA Rules apply to AI.[906] We agree with their assessment and recommendation. Specifically, ePHI, including ePHI in AI training data, prediction models, and algorithm data that is maintained by a regulated entity for covered functions is protected by the HIPAA Rules and all applicable standards and specifications.[907] For example, generative AI tools have produced in their output the names and personal information of persons included in the tools' sources of training data.[908] Similar uses of generative AI by regulated entities, including the training of AI models on patient data, could result in impermissible uses and disclosures, including exposure to bad actors that can exploit the information.[909] As part of its risk analysis and risk management activities, a regulated entity must consider the risk associated with different uses and data.[910] Accordingly, we expect that a regulated entity interested in using AI would include the use of such tools in its risk analyses and associated risk management activities. The regulated entity's risk analysis must include consideration of, among other things, the type and amount of ePHI accessed by the AI tool, to whom the data is disclosed, and to whom the output is provided. The NIST AI Risk Management Framework is a helpful resource for regulated entities to better

[893] Kathryn Marchesini, et al., ''Getting the Best out of Algorithms in Health Care,'' HealthITbuzz, Assistant Secretary for Technology Policy, U.S. Department of Health and Human Services (June 15, 2022), *https://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/getting-the-best-out-of-algorithms-in-health-care.*

[894] *See* Nazish Khalid, et al., ''Privacy-preserving artificial intelligence in healthcare: Techniques and applications,'' Computers in Biology and Medicine, Volume 158, p. 1 (May 2023), *https://www.sciencedirect.com/science/article/pii/S001048252300313X?ref=pdf_download&fr=RR-2&rr=8a7dac430d6d07d5.*

[895] *See* ''Artificial Intelligence Program: Research on AI/[Machine Learning] ML-Based Medical Devices,'' U.S. Food & Drug Administration, U.S. Department of Health and Human Services (June 10, 2024), *https://www.fda.gov/medical-devices/medical-device-regulatory-science-research-programs-conducted-osel/artificial-intelligence-program-research-aiml-based-medical-devices.*

[896] *Id.*

[897] *See* Michael D. Howell, et al., ''Three Epochs of Artificial Intelligence in Health Care,'' Journal of the American Medical Association, Volume 331, Number 3 (Jan. 16, 2024), *https://jamanetwork.com/journals/jama/fullarticle/2813874.*

[898] *See* Aaron A. Tierney, et al., ''Ambient Artificial Intelligence Scribes to Alleviate the Burden of Clinical Documentation,'' New England Journal of Medicine Catalyst (Feb. 21, 2024), *https://catalyst.nejm.org/doi/full/10.1056/CAT.23.0404.*

[899] *Id.*

[900] Julia Adler-Milstein, et al., ''Next-Generation Artificial Intelligence for Diagnosis: From Predicting Diagnostic Labels to 'Wayfinding,''' Journal of the American Medical Association (Dec. 9, 2021), *https://jamanetwork-com.hhsnih.idm.oclc.org/journals/jama/fullarticle/2787207.*

[901] *Id.*

[902] *See* Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 8 (providing NCVHS recommendations to strengthen the HIPAA Security Rule); s*ee also* William Dixon, et al., ''3 ways AI will change the nature of cyber attacks,'' World Economic Forum (June 19, 2019), *https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/.*

[903] ''3 ways AI will change the nature of cyber attacks,'' *supra* note 902.

[904] *Id.*

[905] *Id.*

[906] *Id.*

[907] Where a regulated entity is maintaining ePHI for research purposes as described by 45 CFR 164.512(i), the regulated entity is not performing a covered function.

[908] *See* Jordan Pearson, ''ChatGPT Can Reveal Personal Information From Real People, Google Researchers Show,'' Vice (Nov. 29, 2023), *https://www.vice.com/en/article/chatgpt-can-reveal-personal-information-from-real-people-google-researchers-show/; see also* Bridget McArthur, ''AI chatbot blamed for psychosocial workplace training gaffe at Bunbury prison,'' ABC Southwest (Aug. 20, 2024), *https://www.abc.net.au/news/2024-08-21/ai-chatbot-psychosocial-training-bunbury-regional-prison/104230980.*

[909] *See* Nick Easen, ''Why generative AI presents a fundamental security risk,'' Raconteur (Sept. 9, 2024), *https://www.raconteur.net/technology/why-generative-ai-presents-a-fundamental-security-threat.*

[910] *See* 45 CFR 164.308(a)(1)(ii)(A) and (B); proposed 45 CFR 164.308(a)(2)(i) and (a)(5)(i).

understand, measure, and manage risks, effects, and harms of AI.[911]

The Security Rule requires a regulated entity to conduct repeated risk analyses that consider any changes to its environment or operations, such as updates or changes in technology or clinical administration, and to apply all reasonable updated protections to safeguard ePHI.[912] Accordingly, as technology such as AI evolves, the Department would expect a regulated entity to perform a risk analysis to consider the effects of such changes on the confidentiality, integrity, and availability of ePHI. As NCVHS observed, ''[I]t is important to conduct risk analyses on AI throughout the life cycle of the system.'' [913] We believe the proposals in this NPRM would clarify our expectations for when and how regulated entities need to consider, prepare for, and address such changes. For example, the Department proposes to expressly require that a regulated entity develop a written inventory of its technology assets. Under this proposal, the Department would expect that AI software used to create, receive, maintain, or transmit ePHI or that interacts with ePHI, including where ePHI is used to train the AI software, would be listed as part of its technology asset inventory, which feeds into the regulated entity's risk analysis. Making AI safe and secure with respect to ePHI requires efforts in a variety of areas—biotechnology, cybersecurity, critical infrastructure—to address risks.[914] The Federal Government seeks to ensure that the collection, use, and retention of ePHI is lawful and secure, and that it mitigates privacy and confidentiality risks. Across the administration, Federal agencies are considering potential uses for AI, as well as their benefits and risks, consistent with E.O. 11410 and its principles to advance and govern the development and use of AI.[915] These principles include making AI safe and secure and protecting privacy and civil liberties. For example, the Department finalized regulations earlier this year that improve transparency by health IT developers of certified health IT, including those that are business associates, that supply a particular type of AI—predictive decision support interventions (DSIs).[916] Specifically, the regulations require such health IT developers to provide greater transparency about the design, development, training, evaluation, and use of such predictive DSIs.[917] This approach promotes responsible AI and makes it possible for covered entities to access a consistent, baseline set of information about the algorithms they use to support their decision making and to assess such algorithms for fairness, appropriateness, validity, effectiveness, and safety.[918]

Additionally, the Department proposes to require that regulated entities monitor authoritative sources for known vulnerabilities and to remediate such vulnerabilities in accordance with their patch management program. We also propose to require that patches, updates, and upgrades that address critical and high risks be applied promptly. Together, these proposals would support the rapid response to vulnerabilities that will be necessary as AI becomes more prevalent. Thus, the Department believes that the adoption of the cybersecurity best practices proposed in this NPRM is an important first step to ensuring that AI tools are deployed by regulated entities in a manner that protects the confidentiality, integrity, and availability of ePHI.

3. Virtual and Augmented Reality (VR and AR)

Research on VR and AR technologies is widespread and has produced numerous applications in the health care fields. Such technologies are being used in medical education and patient care, including AR-assisted surgeries, VR-based pain management therapies, and immersive patient education tools.[919] Additionally, innovators are working on ways to incorporate AI with VR and AR for improved diagnostics and treatment planning.[920]

However, as with quantum computing and AI, VR and AR technologies raise new privacy and security concerns. VR and AR involve the use of diverse technologies and the collection of a wide array of sensitive information, including comprehensive biometric data.[921] According to experts, ''[. . .] VR and AR present distinct security challenges, encompassing typical vulnerabilities associated with electronic devices, as well as potential risks of physical harm and leakage of highly sensitive data.'' [922] VR, like any connected computing device, ''is susceptible to standard cybersecurity concerns and various types of cyberthreats, necessitating proactive anticipation.'' [923]

These cybersecurity risks, such as hacking, social engineering, malicious software, and ransomware, can be mitigated through holistic risk analysis and risk management, consistent with the Security Rule administrative standards in 45 CFR 164.308. In addition, patch management,[924] access control,[925] authentication,[926] and appropriate business associate agreements [927] are examples of some of the required safeguards that would apply to VR and AR systems.

We believe the proposals in this NPRM to clarify these safeguards would substantially improve the ability of regulated entities to address these cybersecurity risks. For example, the Department proposes to require that a regulated entity obtains from a business associate written verification that the business associate has deployed the technical safeguards required by the Security Rule, including a written analysis of the business associate's information systems from a person with

[911] ''Artificial Intelligence Risk Management Framework, (AI RMF 1.0),'' NIST AI 100–1, National Institute of Standards and Technology, U.S. Department of Commerce (Jan. 2023), *https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf; see also* ''Joint Guidance on Deploying AI System Securely,'' Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security (Apr. 15, 2024), *https://www.cisa.gov/news-events/alerts/2024/04/15/joint-guidance-deploying-ai-systems-securely.*

[912] 45 CFR 164.508.

[913] *See* Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 8.

[914] 88 FR 75191 (Nov. 1, 2023).

[915] *Id.*

[916] 89 FR 1192 (Jan. 9, 2024).

[917] *Id.*

[918] ''Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing,'' HTI–1 final rule, The Office of the National Coordinator for Health IT, U.S. Department of Health and Human Services (Mar. 7, 2024), *https://www.healthit.gov/topic/laws-regulation-and-policy/health-data-technology-and-interoperability-certification-program#:~:text=ONC%27s%20HTI%2D1%20final%20rule,implementation%20specifications%2C%20and%20certification%20criteria.*

[919] *See* Tarun Kumar Vashishth, et al., ''Virtual Reality (VR) and Augmented Reality (AR) Transforming Medical Applications'' (Oct. 2023), *https://www.researchgate.net/publication/374814301_Virtual_Reality_VR_and_Augmented_Reality_AR_Transforming_Medical_Applications.*

[920] *Id.*

[921] *See* Evangelia Manika, et al., ''AR and VR devices in the healthcare business: legal and ethical challenges,'' International Bar Association (July 6, 2023), *https://www.ibanet.org/AR-VR-devices-in-the-healthcare-business; see also* Sajin Somarajan, ''Minimizing AR/VR Security And Privacy Risks,'' Infosys Digital Experience (accessed July 23, 2024), *https://blogs.infosys.com/digital-experience/mobility/minimizing-ar-vr-security-and-privacy-risks.html.*

[922] *See* ''AR and VR devices in the healthcare business: legal and ethical challenges,'' *supra* note 921; *see also* ''Minimizing AR/VR Security And Privacy Risks,'' *supra* note 921.

[923] *See* ''AR and VR devices in the healthcare business: legal and ethical challenges,'' *supra* note 921; *see also* ''Minimizing AR/VR Security And Privacy Risks,'' *supra* note 921.

[924] *See* proposed 45 CFR 164.308(a)(4)(i).

[925] 45 CFR 164.312(a)(1).

[926] 45 CFR 164.312(d); *see* proposed 45 CFR 164.308(a)(10)(ii)(C) and 164.312(f)(1).

[927] 45 CFR 164.308(b) and 164.314(a).

appropriate knowledge of and experience with generally accepted cybersecurity principles and methods for ensuring the confidentiality, integrity, and availability of ePHI verifying compliance with the requirements of 45 CFR 164.312 and a written certification that the analysis has been performed and is accurate. Under this proposal, a regulated entity would be required to obtain such verification from a business associate-developer of VR/AR software, ensuring that ePHI that is created, received, maintained, or transmitted using the VR/AR software is protected to the same extent as ePHI that is created, received, maintained, or transmitted using other technology assets that are components of the regulated entity's relevant electronic information systems.

Many regulated entities are piloting innovative technologies. Such entities generally have separate departments that research, develop, test, and deploy such technologies.[928] Regulated entities might consider integrating workforce members with expertise in security and privacy into their technology development groups to ensure that privacy and security, including the Security Rule-required safeguards, are embedded into the design of new and emerging technologies.[929] Doing so can help improve security ''while boosting quality, efficiency, and productivity.'' [930]

4. Request for Comment

The Department requests comment on the foregoing discussion of how the Security Rule protects ePHI used in new and developing technologies, including any benefits, drawbacks, or unintended consequences. We also request comment on the following considerations in particular:

a. Whether the Department's understanding of how the Security Rule applies to new technologies involving ePHI is not comprehensive and if so, what issues should also be considered.

b. Whether there are technologies that currently or in the future may harm the security and privacy of ePHI in ways that the Security Rule could not mitigate without modification, and if so, what modifications would be required.

c. Whether there are additional policy or technical tools that the Department may use to address the security of ePHI in new technologies.

[928] *See* Raj Mehta, et al., ''The future of cyber in the future of health. The evolving role of cybersecurity in health care,'' Deloitte (2020), *https://www2.deloitte.com/us/en/pages/advisory/articles/future-of-cybersecurity-healthcare.html.*

[929] *Id.*

[930] *Id.* regarding ''DevSecOps.''

V. Regulatory Impact Analysis

A. Executive Order 12866 and Related Executive Orders on Regulatory Review

The Department of Health and Human Services (HHS or ''Department'') has examined the effects of this proposed rule under Executive Order (E.O.) 12866, Regulatory Planning and Review,[931] E.O. 13563, Improving Regulation and Regulatory Review,[932] E.O. 14094, Modernizing Regulatory Review,[933] the Regulatory Flexibility Act [934] (RFA), the Unfunded Mandates Reform Act of 1995 [935] (UMRA), and E.O. 13132 on Federalism.[936] E.O.s 12866 and 13563 direct the Department to assess all costs and benefits of available regulatory alternatives and, when regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety, and other advantages; distributive effects; and equity). The proposed rule meets the criteria as significant under section 3(f)(1) of E.O. 12866, as amended by E.O. 14094.

The RFA requires us to analyze regulatory options that would minimize any significant effect of a rule on small entities. As discussed in greater detail below, this analysis concludes, and the Secretary certifies, that the notice of proposed rulemaking (NPRM), if adopted, would not result in a significant economic effect on a substantial number of small entities.

The UMRA (section 202(a)) generally requires us to prepare a written statement, which includes an assessment of anticipated costs and benefits, before proposing ''any rule that includes any Federal mandate that may result in the expenditure by State, local, and Tribal governments, in the aggregate, or by the private sector, of $100,000,000 or more (adjusted annually for inflation) in any 1 year.'' [937] The current threshold after adjustment for inflation is $183 million, using the most current (2024) Implicit Price Deflator for the Gross Domestic Product. UMRA does not address the total cost of a rule. Rather, it addresses certain categories of cost, mainly Federal mandate costs resulting from imposing enforceable duties on State, local, or Tribal governments or the private sector; or increasing the stringency of conditions in, or decreasing the funding of, State, local, or Tribal governments under entitlement programs.

This proposed rule, if adopted, would impose mandates that would result in the expenditure by State, local, and Tribal governments, in the aggregate, or by the private sector, of more than $183 million in any one year. The impact analysis in this proposed rule addresses such effects both qualitatively and quantitatively. Each covered entity and business associate (collectively, ''regulated entity''), including government entities that meet the definition of covered entity (*e.g.,* State Medicaid agencies), would be required to: conduct a Security Rule compliance audit; report to covered entities or business associates, as applicable, upon activation of their contingency plan; deploy multi-factor authentication (MFA) in and penetration testing of relevant electronic information systems; complete network segmentation; disable unused ports and remove extraneous software; update cybersecurity policies and procedures; revise business associate agreements; and update workforce training. Business associates would be required to conduct an analysis and provide verification of their compliance with technical safeguards and covered entities would be required to obtain verification from business associates (and business associates from their subcontractors). Additionally, group health plans would need to revise plan documents to require plan sponsors to comply with administrative, physical, and technical safeguards according to the Security Rule standards. Finally, through contractual language, health plan sponsors would need to enhance safeguards for electronic protected health information (ePHI) according to the Security Rule standards. Costs for all regulated entities to change their policies and procedures alone would increase costs above the UMRA threshold in one year, and costs of health plan sponsors would increase total costs further. Although Medicaid makes Federal matching funds available for States for certain administrative costs, these are limited to costs specific to operating the Medicaid program. There are no Federal funds directed at Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliance activities.

The Department believes that pursuant to Subtitle E of the Small Business Regulatory Enforcement

[931] 58 FR 51735 (Oct. 4, 1993).

[932] 76 FR 3821 (Jan. 21, 2011).

[933] 88 FR 21879 (Apr. 11, 2023).

[934] Public Law 96–354, 94 Stat. 1164 (Sept. 19, 1980) (codified at 5 U.S.C. 601–612).

[935] Public Law 104–4, 109 Stat. 48 (Mar. 22, 1995) (codified at 2 U.S.C. 1501).

[936] 64 FR 43255 (Aug. 4, 1999).

[937] Sec. 202 of Public Law 104–4, 109 Stat. 64 (Mar. 22, 1995) (codified at 2 U.S.C. 1532(a)).

Fairness Act of 1996,[938] the Office of Management and Budget's (OMB's) Office of Information and Regulatory Affairs would be likely to determine that when finalized, this rule meets the criteria set forth in 5 U.S.C. 804(2) because it is projected to have an annualized effect on the economy of more than $100,000,000.

The Justification for this Rulemaking and Summary of Proposed Rule Provisions section at the beginning of this preamble contain a summary of this rule and describe the reasons it is needed. We present a detailed analysis below.

1. Summary of Costs and Benefits

The Department identified ten categories of quantifiable costs arising from these proposals that would apply to all regulated entities: (1) conducting a Security Rule compliance audit; (2) obtaining written verification from their business associates or subcontractors that the business associates or subcontractors, respectively, have conducted the required verification of compliance with technical safeguards; (3) notifying other regulated entities when workforce members' access to ePHI is terminated; (4) completing network segmentation; (5) disabling ports and removing extraneous software; (6) deploying MFA; (7) deploying penetration testing; (8) updating policies and procedures; (9) updating workforce training programs; and (10) revising business associate agreements. Additionally, group health plans would be required to update plan documents to require health plan sponsors' compliance with the administrative, physical, and technical safeguards according to the Security Rule and notification of group health plans when health plan sponsors activate their contingency plan. Business associates would have additional obligations to verify compliance with technical safeguards and provide it in writing to covered entities (and subcontractors to business associates) and to notify covered entities upon activation of their contingency plans. Finally, although plan sponsors are not directly subject to the HIPAA Rules, by virtue of the plan document requirements, the Department estimates that certain group health plan sponsors (*e.g.,* employers that provide group health benefits) would likely incur some quantifiable costs to improve safeguards for their electronic information systems that affect the confidentiality, integrity, or availability of ePHI and to notify group health plans upon activation of plan sponsors' contingency plan.

The Department estimates that the first-year costs attributable to this proposed rule total approximately $9 billion. These costs are associated with regulated entities and health plan sponsors engaging in the regulatory actions described above. For years two through five, estimated annual costs of approximately $6 billion are attributable to costs of recurring compliance activities. Table 1 reports the present value and annualized estimates of the costs of this proposed rule covering a 5-year time horizon. Using a 2 percent discount rate, the Department estimates that this proposed rule would result in annualized costs of $6.8 billion for regulated entities and health plan sponsors combined.

TABLE 1—ACCOUNTING TABLE, COSTS OF THE PROPOSED RULE, $ BILLIONS [a]

Costs	Primary estimate	Year dollars	Discount rate	Period covered
Present Value	$34	2023	Undiscounted	2026–2030
Present Value	32	2023	2%	2026–2030
Annualized	7	2023	2%	2026–2030

[a] Figures are rounded.

As a result of the proposed changes in this NPRM, the enhanced security posture of regulated entities would likely reduce the number of breaches of ePHI and mitigate the effects of breaches that nonetheless occur. The Department has partially quantified these effects and presents them in a break-even analysis. The break-even analysis estimates that if the proposed changes in the NPRM reduce the number of individuals affected by breaches by 7 to 16 percent, the revised Security Rule would pay for itself. Alternatively, the same cost savings may be achieved by lowering the cost per affected individual's ePHI by 7 percent ($35) to 16 percent ($82), respectively.

The changes to the Security Rule would likely result in important benefits and some costs that the Department is unable to fully quantify at this time. As explained further below, unquantified benefits include reductions in reputational, financial, and legal harm from breaches of individuals' ePHI, reductions in disruptions to health care delivery, increased confidence among parties to health care business transactions, and improved quality of health care.

TABLE 2—POTENTIAL NON-QUANTIFIED BENEFITS

Benefits [a]
Would benefit individuals by shielding them from unwanted disclosure of their ePHI and resulting reputational, financial, and legal harms from ePHI misuse.
Would reduce reputational damage to regulated entities resulting from breaches.
Would increase confidence among parties to health care business transactions that ePHI is protected to a higher degree than previously.
Would reduce risk of breaches of ePHI by health plan sponsors.
Would help to prevent health care cost increases to recoup financial losses from responding to breaches.
Would help guard against potential data loss.
Would help minimize potential disruption of service for individuals served by any of the affected entities.

[a] Some of the items in this list represent differing perspectives on the same effect. In such cases, if more thorough quantification became feasible, we would take steps to avoid double-counting when summing the quantitative estimates.

[938] Also referred to as the Congressional Review Act, 5 U.S.C. 801 *et seq.*

The Department also recognizes that there may be some costs that are not readily quantifiable, notably, actions that regulated entities may take to comply with existing requirements more fully as a result of proposed clarifications. For example, this would include completing a technology asset inventory, which is a baseline expectation for the existing requirement of conducting a risk assessment; documenting completion of existing requirements; adding more specificity to the required contingency plan, such as designating staff roles with specific responsibilities when a contingency occurs; testing safeguards as part of reviewing and updating policies and procedures and technical controls; and deploying encryption for ePHI in a more concerted manner (including documenting provision of notification in response to individuals' access requests for transmission of ePHI in an unencrypted manner and has been informed of the risks associated with the transmission, receipt, and storage of unencrypted ePHI). These activities are specified in the NPRM, but they would be more in the nature of clarifications to and increased specificity of existing requirements. Because the degree of additional effort by regulated entities to meet these requirements would be dependent on multiple factors and likely to be highly variable, the additional cost is difficult to quantify.

We acknowledge that there may be a small burden associated with documenting that an individual was informed of the risks of unencrypted transmission of ePHI; however, we believe there are few requests that fall into this category. Because we do not have a basis to make an estimate, we have requested data on potential burdens associated with this proposed exception to the proposed standard for encryption in the preamble discussion of 45 CFR 164.312.

The cost of complying with the exceptions to encryption and MFA for medical devices authorized by the U.S. Food & Drug Administration for marketing may depend in part on the extent to which a regulated entity relies on legacy devices because the regulated entity may be required to adopt compensating controls. New devices are likely to have encryption and MFA built into them, not requiring compensating controls. The Department is unable to estimate the range of costs to adopt compensating controls for legacy devices because there is no reliable data to accurately assess the extent to which legacy devices are used in the United States.[939] The Department requests comment on the number of legacy devices in use and the costs of applying compensating controls to such devices.

2. Baseline Conditions

The Security Rule, in conjunction with the Privacy and Breach Notification Rules, protects the privacy and security of individuals' PHI, that is, individually identifiable health information (IIHI). The Security Rule's protections are limited to ePHI, while the Privacy and Breach Notification Rules protect both electronic and non-electronic PHI. The Security Rule establishes standards to protect individuals' ePHI and requires reasonable and appropriate administrative, physical, and technical safeguards. The Security Rule specifies a series of administrative, physical, and technical security requirements that must be performed or implemented for regulated entities to safeguard ePHI. Specifically, entities regulated by the Security Rule must: (1) ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit; (2) protect against reasonably anticipated threats to the security and integrity of the information; (3) protect against reasonably anticipated impermissible uses or disclosures; and (4) ensure compliance by their workforce. A major goal of the Security Rule is protecting the security of individuals' health information while allowing for the development of a health information system to improve the efficiency and effectiveness of the health care system.

The Administrative Simplification provisions of HIPAA (title II) provide the Secretary of HHS with the authority to publish standards for the privacy and security of health information. The Department first proposed standards for the security of ePHI on August 12, 1998, and published a final rule on February 20, 2003. The Department modified the Security Rule in 2013. Recently, as the preamble to this NPRM discusses, changes in the health care environment and insufficient compliance by regulated entities with the existing Security Rule require the modifications proposed here.

For purposes of this Regulatory Impact Analysis (RIA), the proposed rule adopts the list of covered entities (with an updated count) and certain cost assumptions identified in the Department's Information Collection Request (ICR) associated with the HIPAA Privacy Rule to Support Reproductive Health Care Privacy (''2024 ICR'').[940] The Department also relies on certain estimates and assumptions from the 1998 Proposed Rule [941] that remain relevant, the 2003 Final Rule,[942] and the 2013 Omnibus Rule,[943] as referenced in the analysis that follows.

The Department quantitatively analyzes and monetizes the effect that this proposed rule would have on the actions of regulated entities to: conduct a Security Rule compliance audit; provide or obtain verification of business associates' compliance with technical safeguards; notify other regulated entities when workforce members' access to ePHI is altered or terminated; notify covered entities or business associates, as applicable, upon activation of a contingency plan; complete network segmentation; disable unused ports and remove extraneous software; deploy MFA and penetration testing; update health plan documents; update policies and procedures; update workforce training; and revise business associate agreements. The Department also quantitatively analyzes the effects on group health plan sponsors for ensuring that safeguards for their relevant electronic information systems meet Security Rule standards and notifying group health plans upon activation of the plan sponsors' contingency plans.

Additionally, the Department quantitatively analyzes the benefits of the proposed modifications to regulated entities due to an expected reduction in costs of remediation of breaches and risk of breaches by regulated entities.

The Department analyzes the remaining benefits and costs qualitatively because many of the proposed modifications are clarifications of existing requirements and predicting other concrete actions that such a diverse scope of regulated entities might take in response to this rule is inherently uncertain.

Analytic Assumptions

The Department bases its assumptions for calculating estimated costs and benefits on several publicly available datasets, including data from the U.S. Census Bureau (''Census''), the U.S. Department of Labor's (DOL) Bureau of Labor Statistics, the Small Business Administration (SBA), and the Department's Centers for Medicare &

[939] ''Next Steps Toward Managing Legacy Medical Device Cybersecurity Risks,'' *supra* note 742, p. 6.

[940] ''View ICR,'' Office of Information and Regulatory Affairs, Office of Management and Budget (July 9, 2024), *https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=202401-0945-002.*

[941] 63 FR 43242 (Aug. 12, 1998).

[942] 68 FR 8334 (Feb. 20, 2003).

[943] 78 FR 5566 (Jan. 25, 2013).

Medicaid Services (CMS) and Agency for Healthcare Research and Quality (AHRQ). For the purposes of this analysis, the Department assumes that employee benefits plus indirect costs equal approximately 100 percent of pre-tax wages and adjusts the hourly wage rates by multiplying by two, for a fully loaded hourly wage rate. The Department adopts this as the estimate of the hourly value of time for changes in time use for on-the-job activities.

Implementing the proposals likely would require regulated entities to engage workforce members or consultants for certain activities. The Department assumes that an information security analyst would perform most of the activities proposed in the NPRM, consistent with the existing Security Rule requirements. The Department expects that a computer and information systems manager would revise policies and procedures, a training and development specialist would revise the necessary workforce training, a lawyer would revise business associate agreements, and a compensation and benefits manager would revise health plan documents for plan sponsors. To the extent that these assumptions affect the Department's estimate of costs, the Department solicits comment on its assumptions, particularly assumptions in which the Department identifies the level of workforce member (*e.g.,* analyst, manager, licensed professional) that would be engaged in activities and the amount of time that particular types of workforce members spend conducting activities related to this RIA as further described below. Table 3 lists pay rates for occupations referenced in the cost estimates for the NPRM.

TABLE 3—OCCUPATIONAL PAY RATES [944]

Occupation code and title		Fully loaded hourly wage	2023 Average hourly wage
15–1212	Information Security Analysts	$119.94	$59.97
13–1151	Training and Development Specialists	69.20	34.60
11–3111	Compensation and Benefits Manager	145.14	72.57
11–3021	Computer and Information Systems Managers	173.76	86.88
23–1011	Lawyers	169.68	84.84
13–1111	Management Analysts	111.08	55.54
43–0000	Office and Administrative Support Occupations	46.10	23.05

The Department assumes that most regulated entities would be able to incorporate changes to their workforce training into existing cybersecurity awareness training programs and Security Rule training rather than conduct a separate training because the total time frame for compliance from date of publication of a final rule would be 240 days.[945]

Regulated Entities Affected

The changes proposed in this NPRM would apply to covered entities (*i.e.,* health care providers that conduct covered electronic transactions, health plans, and health care clearinghouses) and their business associates (including subcontractors). The Department estimates the number of covered entities to be 822,600 business establishments (see table 4). By calculating costs for establishments, rather than firms,[946] some burdens may be overestimated because certain costs would be borne by a parent organization rather than each separate facility. Similarly, benefits and transfers would be overestimated because entity assumptions flow through to those quantifications. However, decisions about the level of an organization that is responsible for implementing certain requirements likely varies across the health care industry. The Department requests data on the extent to which certain burdens are borne by each facility versus an umbrella organization.

According to Census data,[947] there are 954 Direct Health and Medical Insurance Carrier firms out of a total 5,822 Insurance Carrier firms, such that health and medical insurance firms make up approximately 16.4 percent of insurance firms [= 954/5,822].[948] Also, according to Census data, there are 2,506 Third Party Administration of Insurance and Pension Funds firms and 8,375 establishments. This category also includes clearinghouses. The Department assumes that 16.4 percent of these firms service health and medical insurance because that is equivalent to the share of insurance firms that are health and medical. As a result, the Department estimates that 411 firms categorized as Third Party Administrators are affected by the proposals in this NPRM [= 2,506 × .164]. Similarly, the Department estimates that 1,374 associated establishments would be affected by the proposals in this NPRM [= 8,375 total establishments × .164]. Most of these are business associates. Based on data from the Department's HIPAA audits and experience administering the HIPAA Rules, we are aware of approximately 36 clearinghouses. See table 4 below.

There were 56,289 community pharmacies, including 19,261 pharmacy and drug store firms, operating in the U.S. in 2023.[949] Small pharmacies generally use pharmacy services administration organizations (PSAOs) to provide administrative services, such as conducting negotiations. Based on information from industry, the Department estimates that the proposed rule would affect fewer than 10 PSAOs and we include this within the estimated 1 million business associates affected by the proposals in this NPRM.[950] The Department assumes that

[944] *See* ''Occupational employment and wages—May 2023,'' U.S. Department of Labor, Bureau of Labor Statistics, Table 1. National employment and wage data from the Occupational Employment and Wage Statistics survey by occupation (Apr. 3, 2024), *https://www.bls.gov/news.release/pdf/ocwage.pdf.*

[945] This includes 60 days from publication of a final rule to the effective date and an additional 180 days until the compliance date.

[946] A firm may be an umbrella organization that encompasses multiple establishments.

[947] ''2021 [Statistics of U.S. Businesses] SUSB Annual Data Tables by Establishment Industry,'' United States Census Bureau, U.S. & States, 6-digit NAICS (Dec. 2023), *https://www.census.gov/data/tables/2021/econ/susb/2021-susb-annual.html.*

[948] This percentage was rounded.

[949] *See* ''2023 NCPA Digest, sponsored by Cardinal Health,'' National Community Pharmacists Association, Table 5, p. 9 (2023), *https://www.cardinalhealth.com/content/dam/corp/web/documents/Report/cardinal-health-2023-ncpa-digest.pdf; see also* ''2021 [Statistics of U.S. Businesses] SUSB Annual Data Tables by Establishment Industry,'' *supra* note 947.

[950] *See* Scott Pace, ''The Role and Value of Pharmacy Services Administrative Organizations (PSAOs),'' Impact Management Group, p. 3 (July 20, 2022), *https://content.naic.org/sites/default/files/call_materials/The%20Role%20and%20Value%20of%20Pharmacy%20Services%20Administrative%20July%202022.pdf; see also* ''The Role of Pharmacy Services Administrative Organizations for Independent Retail and Small Chain Pharmacies,'' Avalere Health, p. 4 (Sept. 30, 2021), *https://documents.ncsl.org/wwwncsl/*

Continued

costs affecting pharmacies are incurred at each pharmacy and drug store establishment and each PSAO.

at each pharmacy and drug store establishment and each PSAO.

TABLE 4—ESTIMATED NUMBER, TYPE, AND SIZE THRESHOLD OF COVERED ENTITIES

Covered Entities				
NAICS code	Type of entity	Firms	Establishments	Small business administration (SBA) size threshold [c] (million)
524114	Health and Medical Insurance Carriers	954	5,552	$47
524292	Clearinghouses [a]	36	36	47
622	Hospitals	3,095	7,465	47
446110	Pharmacies [b]	31,671	56,289	37.5
6211–6213	Office of Drs. & Other Professionals	429,476	527,951	9–16
6215	Medical Diagnostic Laboratories & Imaging	8,714	19,477	19–41.5
6214	Outpatient Care	26,084	54,642	19–47
6219	Other Ambulatory Care	10,547	16,114	20.5–40
623	Skilled Nursing & Residential Facilities	42,421	95,175	16–34
6216	Home Health Agencies	27,433	38,040	19
532283	Home Health Equipment Rental	488	1,859	41
Total		580,9198	822,600	

[a] This North American Industry Classification System (NAICS) category includes clearinghouses and is titled ''Third Party Administration of Insurance and Pension Funds.'' The number of clearinghouses is based on the Department's research.

[b] Number of pharmacies is taken from industry statistics.

[c] *See* ''Table of Small Business Size Standards,'' U.S. Small Business Administration (Mar. 17, 2023), *https://www.sba.gov/sites/sbagov/files/2023-06/Table%20of%20Size%20Standards_Effective%20March%2017%2C%202023%20%282%29.pdf.* The SBA size thresholds are discussed in Section V.C. Regulatory Flexibility Act—Small Entity Analysis of this NPRM.

The Department also estimated the percentage of rural and urban health care providers by matching health care provider data from CMS,[951] Health Resources & Services Administration,[952] and the Statistics of U.S. Businesses (SUSB) [953] with county population data from the U.S. Census Bureau.[954] We determined whether a health care provider was rural or urban based on OMB's standards for delineating metropolitan and micropolitan statistical areas.[955] Consistent with OMB's standard, we considered a county to be rural if it has fewer than 50,000 inhabitants.[956] This includes micropolitan areas (towns and cities between 10,000 and 49,999) and counties outside of metropolitan statistical areas and micropolitan areas. Based on this analysis, we estimate that 7–8 percent of health care providers operate in rural areas.

Estimated Number and Type of Business Associates

The Department adopts the estimate of approximately 1,000,000 business associates (including subcontractors) as stated in the 2024 ICR and the 2013 ''Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health [HITECH] Act and the Genetic Information Nondiscrimination Act, and Other Modifications to the HIPAA Rules'' final rule.[957] We considered whether to increase this figure in our updates but did not do so because many business associates serve multiple covered entities. We lack sufficient data to estimate the number of such businesses more precisely, but we believe that the number of business associates is highly dynamic and dependent on multiple market factors, including expansion and consolidation among various lines of business, changing laws and legal interpretations, and emerging technologies. We include subcontractors of business associates within our estimate because they are business associates of business associates.

The Department welcomes comments on the number or type(s) of regulated entities that would be affected by the proposals in this proposed rule and the extent to which they may experience costs or other burdens not already accounted for in the cost estimates. The Department also requests comment on the number of health plan documents that would need to be revised, if any. The Department additionally requests detailed comment on any situations, other than those identified here, in which covered entities or business associates would be affected by the proposals in this rulemaking.

Health Plan Sponsors

Within this NPRM, the Department is for the first time including estimates of health plan sponsors' potential costs of compliance with specific

Foundation/sponsor-views/The_Role_of_PSAOs_Independent_Pharmacies.pdf.

[951] *See* ''Provider of Services File—Internet Quality Improvement and Evaluation System—Home Health Agency, Ambulatory Surgical Center, and Hospice Providers,'' Centers for Medicare & Medicaid Services (2024), *https://data.cms.gov/provider-characteristics/hospitals-and-other-facilities/provider-of-services-file-internet-quality-improvement-and-evaluation-system-home-health-agency-ambulatory-surgical-center-and-hospice-providers;* ''Provider of Services File—Hospital & Non-Hospital Facilities,'' Centers for Medicare & Medicaid Services (2024), *https://data.cms.gov/provider-characteristics/hospitals-and-other-facilities/provider-of-services-file-hospital-non-hospital-facilities.*

[952] *See* ''Area Health Resources Files,'' Health Resources & Services Administration, U.S. Department of Health and Human Services (2022–2023 County Level Data), *https://data.hrsa.gov/data/download?data=AHRF#AHRF.*

[953] *See* ''2021 [Statistics of U.S. Businesses] SUSB Annual Data Tables by Establishment Industry,'' *supra* note 947.

[954] *See* ''Delineation Files,'' U.S. Census Bureau, U.S. Department of Commerce (2023), *https://www.census.gov/geographies/reference-files/time-series/demo/metro-micro/delineation-files.html.*

[955] *See generally* 86 FR 37770 (July 16, 2021).

[956] *See* 86 FR 37770, 37778 (July 16, 2021).

[957] 78 FR 5565 (Jan. 25, 2013).

administrative, physical, and technical safeguards of the Security Rule. The Department relied on data from AHRQ and the U.S. Census to estimate the number of firms offering group health plans (1.9 million),[958] and multiplied that by the percentage that offer at least one self-insured plan to calculate the number of plan sponsors that would be likely to receive ePHI and be subject to the requirements of 45 CFR 164.314(b) [1,943,484 × .382 = 742,411]. We solicit comments on whether group health plans or third-party administrators address any Security Rule requirements for plan sponsors, so the plan sponsors would not have an additional burden or would have a smaller burden than estimated below.

Individuals Affected

The number of individuals potentially affected by the proposed changes to the Security Rule includes most of the United States population (approximately 337 million), specifically those who have received any health care in the past seven years and whose ePHI is likely created, received, maintained, or transmitted by a regulated entity. Statistics about the number of individuals affected by breaches of PHI provide insight into known instances where safeguards were breached, although the effects of the Security Rule extend farther than that, to all ePHI. Data from the 2022 Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Year 2022 [959] revealed nearly 42 million individuals affected by breaches of PHI in that year. Third-party sources reported approximately 133 million individuals affected by health care breaches in 2023.[960] According to UnitedHealth Group, the 2024 breach of its clearinghouse subsidiary Change Healthcare may have affected approximately one-third of the U.S. population, or 112 million individuals.[961] The Department believes that the range of individuals potentially affected by the proposed regulatory changes would be from 42 million to 337 million.

HIPAA Breach Data

The Department has reported HIPAA/HITECH breach data annually since 2009. Table 5 shows the data as reported to Congress for the past five years. We relied on this data, combined with breach cost data from industry sources, to analyze the potential savings of the NPRM.

TABLE 5—BREACHES OF PHI

Year	Small breaches (fewer than 500 affected individuals)		Large breaches (500+ affected individuals)		Total	
	Breach count	Affected individuals	Breach count	Affected individuals	Breach count	Affected individuals
2018	63,098	296,948	302	12,196,601	63,400	12,493,549
2019	62,771	284,812	408	38,732,966	63,179	39,017,778
2020	66,509	312,723	656	37,641,403	67,165	37,954,126
2021	63,571	319,215	609	37,182,558	64,180	37,501,773
2022	63,966	257,105	626	41,747,613	64,592	42,004,718

3. Costs of the Proposed Rule

Below, the Department provides the basis for its estimated quantifiable costs resulting from the proposed changes to specific provisions of the Security Rule. Many of the estimates are based on assumptions formed through OCR's experience with compliance and enforcement and accounts from stakeholders. For each cost, the Department provides its main estimate, as well as additional high and low estimates for some costs to account for any uncertainty in the compliance approach of regulated entities.

All estimates in this section are based on subject matter expertise. The Department requests information or data points from commenters to further refine its estimates and assumptions.

a. Costs Associated With Conducting a Security Rule Compliance Audit

The Department estimates that all regulated entities would need to conduct a Security Rule Compliance Audit because this would be a new requirement under proposed 45 CFR 164.308(a)(14). Although some regulated entities have mistakenly conducted such an audit in lieu of a risk analysis, the Department believes that costs for the compliance audit as a separate requirement should be attributed to the proposed changes in the NPRM. Further, because this would be an annual requirement, the Department is including this as a recurring cost. The Department estimates that regulated entities would need an average of 2 hours of labor by an information systems analyst to conduct the compliance audit, based on the assumption that regulated entities have already documented Security Rule compliance activities as currently required. This would result in total estimated costs of $437,205,288 [= 1,822,600 regulated entities × 2 hours × $119.94]. The respective low and high estimates would be 0.25 and 2.5 hours of information systems analyst labor, resulting in respective total estimated costs of $54,650,6611 [= 1,822,600 regulated entities × 0.25 hours × $119.94] and $546,506,610 [= 1,822,600 regulated entities × 2.5 hours × $119.94].

[958] *See* ''Medical Expenditure Panel Survey—Insurance Component,'' Tables I.A.1 and I.A.2, Agency for Healthcare Research and Quality (2023), *https://meps.ahrq.gov/data_stats/summ_tables/insr/national/series_1/2023/ic23_ia_g.pdf?_gl=1*16xft35*_ga*MTE0MDI5NzI0LjE3MDk2NjQ0NDM.*_ga_45NDTD15CJ*MTczMTEwMzQ4OS4yLjEuMTczMTEwMzUzNS4xNC4wLjA* (showing the number of establishments and percent offering health plans) and ''County Business Patterns: 2021,'' United States Census Bureau (April 27, 2023), *https://www.census.gov/data/datasets/2021/econ/cbp/2021-cbp.html* (providing the ratio of firms to establishments). We assume one health plan sponsor per firm that offers a self-insured group health plan.

[959] *See* ''Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Year 2022,'' *supra* note 213, p. 9 (2023).

[960] *See* Steve Alder, ''December 2023 Healthcare Data Breach Report,'' The HIPAA Journal (Jan. 18, 2024), *https://www.hipaajournal.com/december-2023-healthcare-data-breach-report/*.

[961] *See* ''What We Learned: Change Healthcare Cyber Attack,'' U.S. House of Representatives Committee on Energy & Commerce (May 3, 2024), *https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack*.

b. Estimated Costs From Adding a Requirement for Business Associates to Analyze Compliance With Technical Safeguards

For proposed 45 CFR 164.308(b), the Department estimates that business associates that handle ePHI would need to spend an average of 2 hours (with a low estimate of 0.25 hours and high estimate of 2.5 hours) analyzing how their cybersecurity measures comply with the proposed requirements for technical safeguards and producing a verification report for covered entities at the hourly wage rate of an information security analyst. This estimate assumes that business associates have already documented existing safeguards, policies, and procedures, so that the costs attributable to the new requirement are incremental and would total approximately $239,880,000 [1 million business associates × 2 hours × $119.94], with a low estimate of $29,985,000 [1 million business associates × 0.25 hours × $119.94] and high estimate of $299,850,000 [1 million business associates × 2.5 hours × $119.94].

c. Costs Arising From Covered Entities and Business Associates Obtaining Verification From Business Associates of Compliance With Technical Safeguards

Under 45 CFR 164.308(b), the Department further estimates that each covered entity would need to spend an average of 30 minutes (with 15 minutes as a low estimate and 90 minutes as a high estimate) requesting and obtaining compliance reports from its business associates about their deployment of technical safeguards required by the Security Rule at the hourly wage of an information security analyst. This assumes that in most instances, business associates would produce the required verification for covered entities without being prompted by a request because they would be required to do so by the Security Rule, as proposed in the NPRM. It further assumes that covered entities have readily available means of contacting business associates, such as via email, and that the contact could be a single email draft sent in a batch. The average time burden per entity depends on verification frequency, likely influenced by entities' average number of business associates and how frequently entities change business associates. The low estimate assumes that entities verify less frequently, whereas the high estimate assumes entities verify more frequently. At the wage rate of an information security analyst, this would result in estimated total costs for covered entities of $49,331,322 [= 822,600 covered entities × 0.5 hours × $119.94], with a low estimate of $24,665,661 [= 822,600 covered entities × 0.25 hours × $119.94] and high estimate of $147,993,966 [= 822,600 covered entities × 1.5 hours × $119.94].

The proposed requirement to obtain verification of compliance with technical safeguards also would apply to business associates with respect to their subcontractors. However, we believe that a much smaller number of business associates rely on subcontractors compared to the number of covered entities that rely on business associates to conduct activities on their behalf. Thus, we estimate that, on average, business associates would need 5 minutes annually to obtain verification from their subcontractors that the subcontractors have complied with technical safeguards as required by the Security Rule. The estimate includes only the time needed for business associates to send a mass email to subcontractors because we have already addressed the burden on business associates of producing the verification in the previous section and that estimate includes burdens on subcontractors. The high estimate for this activity would be an average of 15 minutes per business associate, and a low estimate would be for business associates to 2 minutes on this activity. At the wage rate of an information security analyst, this would add estimated total costs for business associates of $9,995,000 [= 1,000,000 business associates × 0.083 hours × $119.94], with a high estimate of $29,985,000 [= 1,000,000 business associates × .25 hours × $119.94].

d. Cost Related to Notification of Termination or Change of Workforce Members' Access to ePHI

The Department estimates that regulated entities are likely to incur additional costs to implement a process to notify other regulated entities when a workforce member's access to ePHI is terminated or changed under proposed 45 CFR 164.308(a)(9)(ii). This estimate assumes that notifications will take an average of 1 hour annually per regulated entity. This results in new estimated costs totaling $84,021,860 [= 1,822,600 regulated entities × 1 hour × $46.10].[962]

e. Cost Related to Regulated Entities Deploying Multi-Factor Authentication

The Department estimates that, on average, regulated entities would have an information security analyst spend 1.5 hours deploying MFA, as specifically required under proposed 45 CFR 164.312(f)(2)(ii). This would be a one-time, first-year burden that includes an average of 30 minutes for a regulated entity to select an MFA solution that allows them to meet the requirements of the proposal without creating workflow disruptions or delays. This estimate would vary depending on how prevalent MFA is in the industry when and if the requirements of the NPRM are finalized. As a widely accepted information security practice, the Department believes that many large entities have already deployed MFA and the costs range from zero to only a few dollars per user. The low estimate would be 01 hours on average (assuming that many entities already have some form of MFA), and the high estimate would be 1.75 hours (assuming that few entities have MFA). At the loaded wage rate of an information security analyst, the total estimated cost would be $327,903,966 [= 1,822,600 regulated entities × 1.5 hours × $119.94], with a low estimated total of $218,602,644 [= 1,822,600 regulated entities × 1 hour × $119.94] and a high estimated total of $382,554,627 [= 1,822,600 regulated entities × 1.75 hours × $119.94]. The Department applies this cost in the first year only because minimal additional labor is needed to maintain this safeguard once it has been deployed.

f. Costs Related to Network Segmentation

The Department believes that most large regulated entities and many medium-sized regulated entities have segmented their information networks to some degree; however, additional actions may be needed to more fully protect ePHI as required under proposed 45 CFR 164.312(a)(2)(vi). Further, small entities may not have been aware of the importance of segmenting networks or taken steps to segment their networks. The Department estimates that each regulated entity would spend an average of 4.5 hours to set up network segmentation in the first year of compliance with a final rule (with a low estimate of 4 hours and a high estimate of 5 hours) at the hourly wage of an information security analyst. The Department further assumes that in the following years, the burden to maintain the segmented network would be minimal and incorporated into the maintenance requirements. The total first year estimated cost of the network segmentation requirement would be $983,711,898 [= 1,822,600 regulated entities × 4.5 hours × $119.94] with a low estimated total of $874,410,576 [= 1,822,600 regulated entities × 4 hours ×

[962] *See* table 3, wage rate for Office and Administrative Support Occupations.

$119.94] and a high estimate of $1,093,013,220 [= 1,822,600 regulated entities × 5 hours × $119.94].

g. Cost Related to Disabling Ports and Removing Extraneous Software

The Department believes that large regulated entities have already disabled unused network ports and removed extraneous software as part of existing configuration requirements. However, the Department believes that small and medium-sized regulated entities are less likely to have performed these actions and thus would incur a new burden to implement these aspects of configuration management proposed at 45 CFR 164.312(c)(2)(ii) and (iv). The Department estimates that 629,796 establishments are owned by small and medium-sized covered entities,[963] which is approximately 76.56 percent of all covered entities [= 629,796/822,600]. The Department applies that percentage to the estimated number of business associates [= 0.7656 × 1,000,000] to arrive at the estimated number of regulated entities with quantifiably increased burdens from these proposed requirements to disable unused ports and remove extraneous software. We estimate that for these 1,395,396 regulated entities [= 629,796 covered entities + 765,600 business associates], an average annual burden of 30 minutes would be needed at the wage rate of an information security analyst to make needed changes to configuration management, specifically disabling unused ports and removing extraneous software. This would result in estimated total cost increases of $83,681,898 [= 1,395,3960 regulated entities × 0.5 hours × $119.94], with a low estimate of $41,840,949 [= 1,395,396 regulated entities × 0.25 hours × $119.94] based on an estimated annual burden of 15 minutes per affected entity and a high estimate of $109,301,322 [= 1,822,600 regulated entities × 0.50 hours × $119.94] based on an estimated annual burden of 30 minutes for all regulated entities.

h. Costs Related to Regulated Entities Conducting Penetration Testing

The Department estimates that each regulated entity would spend an average of 3 hours conducting penetration testing (with a low estimate of 2 hours and a high estimate of 10 hours) at the hourly wage of an information security analyst. The Department expects that there might be a high degree of variability between entities depending on their size and technological sophistication. Large entities have more endpoints to test, and thus have greater exposure. The Department also believes there is room for significant variability in the effort that regulated entities may apply to this activity. At the wage rate of an information security analyst, this would result in estimated total annual costs for regulated entities of $655,807,932 [= 1,822,600 regulated entities × 3 hours × $119.94], with a low estimated total of $437,205,288 [= 1,822,600 regulated entities × 2 hours × $119.94] and high estimated total of $2,186,026,440 [= 1,822,600 regulated entities × 10 hours × $119.94].

i. Costs Arising From Reporting Contingency Plan Activation

The Department estimates that business associates would need to notify other regulated entities in the event that they activate their contingency plan once business associate agreements are revised according to proposed 45 CFR 164.314(a)(2)(i)(D). The Department believes this is unlikely to occur more frequently than once per year and that the time to do so would be minimal because the proposed requirement does not specify the means or scope of such notification. The Department estimates that business associates would need an average of 30 minutes (with 15 minutes as a low estimate and 45 minutes as a high estimate) to report to other regulated entities, as applicable, when their contingency plan is activated at the wage rate of an information security analyst for a total annual cost of $59,970,000 [= 1,000,000 business associates × 0.5 hours × $119.94], with a low estimated total of $29,985,000[= 1,000,000 business associates × 0.25 hours × $119.94] and high estimated total of $89,955,000 [= 1,000,000 business associates × 0.75 hours × $119.94].

j. Revised Health Plan Documents

The Department estimates that health care insurers and third-party administrators would need to revise health plan documents to reflect that health plan sponsors that receive ePHI (that is not limited to summary health information or disenrollment information) are protecting ePHI with the administrative, physical, and technical safeguards detailed in the Security Rule, as proposed. These 6,162 entities collectively would be responsible for updating approximately 742,411 health plan documents at the wage rate of a compensation and benefits manager. The Department's estimate assumes that on average each plan document requires 30 minutes to update for a total estimated cost of $53,876,766 [1742,411 × 0.5 hours × $145.14]. The Department has attributed these costs solely to health plans and not health plan sponsors because the health plan is the regulated entity.

k. Estimated Costs for Developing New or Modified Policies and Procedures

The Department anticipates that regulated entities would need to develop new or modified policies and procedures for the proposed new requirements to obtain or provide verification of business associates' compliance with the Security Rule's requirements for technical safeguards, conducting a Security Rule compliance audit, and reporting the activation of a contingency plan, as well as other proposed changes, depending on the regulated entities' existing policies and procedures. The Department estimates that the costs associated with developing such policies and procedures would be the labor of a computer and information systems manager for an average of 3.5 hours (with 2.5 hours as a low estimate and 6 hours as a high estimate, depending on the number of entities with written policies and procedures, and their degree of specificity). This would result in total annual costs of $1,108,432,416 [= 1,822,600 regulated entities × 3.5 hours × $173.76], with a low estimated total of $791,737,440 [= 1,822,600 regulated entities × 2.5 hours × $173.76] and high estimated total of $1,900,169,856 [= 1,822,600 regulated entities × 6 hours × $173.76]. The existing rule requires updates to policies and procedures in response to environmental or operational changes affecting the security of the ePHI, and as a result, the Department is estimating additional costs for new policies related to this proposed rule as an incremental increase.

l. Costs Associated With Training Workforce Members

The Department anticipates that regulated entities would be able to incorporate new content into existing Security Rule training programs and that the costs associated with doing so would be attributed to the labor of a training specialist for an estimated 2 hours for total annual costs of $252,247,840 [= 1,822,600 regulated entities × 2 hours × $69.20]. The low estimate for this activity is $126,123,920 [= 1,822,600 regulated entities × 1 hour × $69.20], and the high estimate is $378,371,760 [= 1,822,600 regulated entities × 3 hours × $69.20]. Many of the changes in the NPRM require the

[963] As defined by having 500 or fewer employees. *See* ''2021 [Statistics of U.S. Businesses] SUSB Annual Data Tables by Establishment Industry,'' *supra,* note 947.

adoption of standard cybersecurity practices as applied specifically to address the confidentiality, integrity, and availability of ePHI, so we expect that an information security analyst would be familiar with this content. These estimated costs would address any required revisions to training for workforce members within the first year of compliance with a final rule. Any further recurring component is likely to be implemented into regularly scheduled employee training and thus would not be directly attributable to the proposals in this NPRM.

m. Revising Business Associate Agreements

The NPRM proposes to provide a transition period in proposed 45 CFR 164.318 for regulated entities to revise business associate agreements to comply with the proposed changes to the requirements of the Security Rule. The proposed transition period would allow regulated entities to revise existing agreements by the earlier of the contract renewal date that falls after the compliance date of a final rule, or within one year of the rule's effective date. For a large share of existing agreements, this would allow regulated entities to complete the revisions on a rolling basis according to the dates they are renewed. The Department estimates that 1,822,600 [964] business associate agreements would need to be revised if this NPRM is adopted and that, on average, the portion of this activity that results from the rule's modifications would take an hour of a lawyer's time for each regulated entity. This would result in annual costs of $309,258,768 [= 1,822,600 regulated entities × 1 hour × $169.68]. The Department recognizes that this estimate may not fully account for all revised business associate agreements. However, the Department believes that in some instances, one hour of time is more than would be needed. We also believe it is likely that, for some regulated entities, a professional other than a lawyer would be responsible for the revised agreements at a lower hourly wage. For some large business associates, the Department believes that a single agreement is used for most of its customers. The Department's estimates assume that most agreements would be revised within the first year and accounts for all of them within that time period. This would be considered a one-time cost; in other words, it is not carried over into future years. As with all the estimates in this NPRM, the Department invites comments about the assumptions underlying the proposed cost projections.

n. Plan Sponsors' Obligations

Proposed 45 CFR 164.314(b)(2) would mandate that group health plan documents require their health plan sponsors who receive ePHI that is not limited to summary health information or enrollment or disenrollment information to deploy the administrative, physical, and technical safeguards for ePHI required by the Security Rule and notify their group health plans upon activation of the plan sponsors' contingency plan. Currently, plan documents must require such health plan sponsors to have safeguards in place, but not necessarily the safeguards specified in the Security Rule.[965] The Department estimates that an additional 52.42 hours of labor would be needed for each affected health plan sponsor to bring its security safeguards for ePHI into compliance with the Security Rule standards and to notify group health plans when its contingency plan is activated, over and above the actions attributable to safeguards already in place for ePHI and for sponsors' electronic information systems generally. The Security Rule compliance activities attributed to group health plan sponsors are shown in table 7, below.

Most compliance activities would be performed by a workforce member at the hourly wage rate of an information security analyst ($119.94), while documentation of maintenance would be performed at the rate of a management analyst ($111.08) and notification of termination or change of workforce members' access to ePHI would be performed by an office administrative assistant ($46.10). This would result in estimated total first year costs for health plan sponsors of $4,658,781,219 as shown in detail in table 7.

o. Total Quantifiable Costs

The Department summarizes in tables 6 and 7 the estimated costs that regulated entities (approximately $4,655 million) and plan sponsors (approximately $4,659 million), respectively, would experience in the first year of implementing the proposed regulatory changes. The Department anticipates that these costs would be for the following activities: conducting a Security Rule compliance audit; obtaining verification of business associates' and subcontractors' compliance with technical safeguards; providing verification of business associates' compliance with technical safeguards; providing notification of termination or change of workforce members' access to ePHI; deploying MFA and penetration testing; segmenting networks; disabling unused ports; removing extraneous software; notifying covered entities or business associates, as applicable, upon activation of a contingency plan; and updating health plan documents, policies and procedures, workforce training, and business associate agreements. These costs would also include health plan sponsors deploying safeguards for their relevant electronic information systems to meet Security Rule standards and notifying group health plans upon activation of a plan sponsor's contingency plan.

TABLE 6—FIRST YEAR COST ESTIMATES FOR REGULATED ENTITIES' PROPOSED COMPLIANCE OBLIGATIONS [a]

Compliance activities	Burden hours × frequency	Respondents	Wage rate	Total annual cost (millions)
Security Rule Compliance Audit	2 × 1	1,822,600 Regulated Entities	$119.94	$437
BA Verification of Technical Safeguards	2 × 1	1,000,000 Business Associates	119.94	240
Obtain BA Compliance Verification	.5 × 1	822,600 Covered Entities	119.94	49
Obtain Subcontractors' Compliance Verification.	.083 × 1	1,000,000 Business Associates	119.94	10
Notification of Workforce Members' Termination of access to ePHI.	1 × 1	1,822,600 Regulated Entities	46.10	84

[964] This is the estimated total number of covered entities and business associates.

[965] *See* 45 CFR 164.314(b) (requiring that a group health plan ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan).

TABLE 6—FIRST YEAR COST ESTIMATES FOR REGULATED ENTITIES' PROPOSED COMPLIANCE OBLIGATIONS [a]—Continued

Compliance activities	Burden hours × frequency	Respondents	Wage rate	Total annual cost (millions)
Multi-factor Authentication	1.5 × 1	1,822,600 Regulated Entities	$119.94	$328
Network Segmentation	4.5 × 1	1,822,600 Regulated Entities	119.94	984
Configuration Management	.5 × 1	1,395,396 Regulated Entities	119.94	84
Penetration Testing	3 × 1	1,822,600 Regulated Entities	119.94	656
Notification of Contingency Plan Activation	.5 × 1	1,000,000 Business Associates	119.94	60
Update Health Plan Documents	.5 × 120	3,102,851 Health Plan Documents	145.14	54
Update Policies and Procedures	3.5 × 1	1,822,600 Regulated Entities	173.76	1,108
Update Workforce Training	2 × 1	1,822,600 Regulated Entities	69.20	252
Revise Business Associate Agreements	1 × 1	1,822,600 Regulated Entities	169.68	309
Total Annual Cost Burden				4,655

[a] These represent first year estimated costs and are rounded.

The Department presents the estimated cost of health plan sponsors' compliance with the proposed new requirements in table 7 below.

TABLE 7—FIRST YEAR COST ESTIMATES OF HEALTH PLAN SPONSORS' PROPOSED COMPLIANCE OBLIGATIONS [a]

Compliance activities	Burden hours × frequency	Respondents	Wage rate	Total annual cost (millions)
Risk Analysis—Documentation	5 × 1	742,411 Plan Sponsors	$119.94	$445
Information System Activity Review—Documentation.	.75 × 12	742,411 Plan Sponsors	119.94	801
Ongoing Education	.17 × 12	742,411 Plan Sponsors	119.94	178
Security Incidents (other than breaches)—Documentation.	2 × 12	742,411 Plan Sponsors	119.94	2,137
Contingency Plan—Testing and Revision	2 × 1	742,411 Plan Sponsors	119.94	178
Contingency Plan—Criticality Analysis	.5 × 1	742,411 Plan Sponsors	119.94	45
Notification of Workforce Members' Termination of ePHI Access.	.25 × 1	742,411 Plan Sponsors	46.10	9
Maintenance Records	.5 × 12	742,411 Plan Sponsors	111.08	495
Multi-factor Authentication	1.5 × 1	742,411 Plan Sponsors	119.94	133
Configuration Management	.5 × 1	742,411 Plan Sponsors	119.94	45
Penetration Testing	2 × 1	742,411 Plan Sponsors	119.94	178
Notification of Contingency Plan Activation	.17 × 1	742,411 Plan Sponsors	119.94	15
Total Annual Cost Burden				4,659

[a] These represent first year estimated costs and are rounded.

Together, regulated entities' and affected health plan sponsors' estimated first year costs of compliance with the proposals in the NPRM would be approximately 9,314 million (or $9 billion).

p. Costs Borne by the Department

The covered entities that are operated by the Department would be affected by the changes in a similar manner to other covered entities, and such costs have been factored into the estimates above. The Department has not identified other costs to the Department related to the changes in the NPRM. A reduction in the number of large breaches (affecting 500 or more individuals per incident) would benefit the Department by enabling it to focus its resources on a smaller number of breach investigations, and potentially resolve such investigations more quickly.

4. Benefits of the Proposed Rule

a. Quantitative Analysis of Benefits

A key goal of strengthening the cybersecurity posture of regulated entities is to reduce the number and severity of security incidents, including breaches of ePHI. The Department believes that compliance with the proposed changes, which align with industry guidelines and best practices, would benefit regulated entities by reducing the cost of breaches. Although the costs of implementing the proposed cybersecurity measures would be significant, the costs of responding to breaches of ePHI are much higher. According to industry data, the average cost of a health care breach in 2023 rose to $10.93 million, the highest among all industries studied,[966] and the per record cost of a breach involving personally identifiable information (across all industries) was $183.[967] These costs include detection and investigation activities, notification activities, post-breach response activities, and activities attempting to minimize the loss of business. Thus, the benefits of the proposed rule would be to reduce the harms of health care breaches described in the preamble. The Department believes that implementing the changes in the NPRM would reduce both the incidence of breaches in health care and the costs of mitigating breaches when they occur.

The Department also analyzed the potential cost savings of proposals that

[966] *See* ''Cost of a Data Breach Report 2023,'' *supra* note 131, p. 13.

[967] *Id.* at 18.

correspond to major factors affecting the costs of large breaches as identified in published reports.[968] The Department estimates that, at a minimum, performing the following actions would quantifiably reduce costs: (1) encryption; (2) penetration testing; (3) requiring MFA and notification of termination of access to ePHI; (4) increasing employee training; and (5) reducing noncompliance with regulations. These factors would account for an estimated 23.6 percent decrease in large breach costs.[969] For health care breaches, this corresponds to an estimated cost savings of $2.6 million per large breach in high incidence years, and $2.1 million per large breach in low incidence years.

Non-Quantitative Analysis of Benefits

A fundamental benefit of the proposed rule would be to decrease the effects of breaches on individuals who are the subjects of ePHI, namely patients and health plan members. Breaches of ePHI may cause harm to individuals in many ways, including loss of reputation and personal dignity and financial and medical fraud, which may result in false debts, impaired credit, and even health threats from misuse of health insurance credentials by another individual. ''[H]ealthcare data, which includes medical histories and personal identification, can last a lifetime. The information collected can be used for ransom, to commit tax frauds, to provide supporting disability documentation, to send fake bills to insurance providers, to obtain healthcare, prescription drugs, medical treatment, and to obtain government benefits like Medicare and Medicaid.'' [970] Hackers can use stolen personal, medical, and financial data to take out a bank loan in the victim's name and change direct deposit information in payroll systems, allowing them to steal wages as well.[971] In addition, medical identity fraud can impact the victim's credit score and health insurance premiums, and may result in unexpected legal fees.[972] Medical identity fraud also enables thieves to obtain medical treatment using the victim's stolen ePHI. This can lead to the thief's medical conditions being incorporated into the victim's medical records and impacting the victim's ability to receive appropriate medical treatment based on accurate records in the future, or any care at all depending on whether the thief has exhausted the victim's insurance benefits.[973] Overall, recovering compromised ePHI and addressing the consequences of breached information can be a long and arduous process that can cost victims large amounts of time, energy, and money.[974]

Breaches of ePHI maintained by health care systems can also pose a threat to the medical well-being of affected individuals. Cyberattacks on health care organizations can include the deployment of malware that compromises the function of both internal and external medical devices. Such software can alter the dosages of sensitive medicines or shut down devices while they are in use, thus affecting patient care.[975] Some of the medical devices that are vulnerable to malicious software attacks include insulin pumps and cardiac implant devices.[976] The consequences of a cyberattack on such a medical device can be fatal.

Cyberattacks on relevant electronic information systems also hinder the efficiency of hospitals and limit the quality of care provided to patients. Breaches of relevant electronic information systems negatively affect the routine functions of health care organizations. They can affect the availability of ePHI and relevant electronic information systems and redirect critical resources from patient care to addressing the cybersecurity attack. A 2020 cyberattack on a large covered entity disrupted communication and clinician access to medical records, including to individualized chemotherapy plan templates and tools for communicating during treatment preparation and delivery.[977] In the first week following the attack, the hospital's ability to provide critical outpatient care was reduced by 40 percent and infusion visit volume decreased by 52 percent. Many patients had to be transferred to other sites to minimize delays in receiving critical medications. The effects of this data breach are not unique to this provider. There is evidence that cyberattacks on health care organizations decrease the number of patients they are able to treat in a given day and staff utilization.[978] Decreases in efficiency and number of treated patients also cause health care facilities to lose revenue because of their inability to provide care during a cybersecurity event.

Similar to the effects of breaches of ePHI on individuals, health care organizations and facilities also experience reputational and financial impacts because of cybersecurity attacks. Hospitals can lose the community's trust and be subject to lawsuits from individuals whose data was compromised.[979] Organizations that experience cybersecurity attacks can experience reputational harm and other monetary costs, such as those associated with providing breach notifications, paying fines to regulators and damages to individuals, and providing credit monitoring and identity theft-related services.[980] The harm to an organization's reputation is difficult to quantify, but it can also affect the quality of care administered to individuals.[981] Privacy and security of ePHI are paramount to individuals feeling safe and at ease sharing their IIHI with clinicians. Security breaches can negatively impact a patient's confidence in a health care organization if they believe their information and privacy may be compromised. This can cause them to delay seeking treatment or

[968] The impact factor costs and cost savings are based on estimates for all breaches from the annual IBM Security and Ponemon Institute Costs of a Data Breach Reports for years 2018–2023. *See id.* at p. 28.

[969] The Department calculated the percentage decrease as a share of the sum of factor costs from the average breach cost: ($218,915 + $180,358 + $187,703 + $221,593 + $232,867)/$4,450,000 = 0.236.

[970] *See* ''New Dangers in the New World: Cyber Attacks in the Healthcare Industry,'' *supra* note 135, p. 3.

[971] *See* ''Is the HIPAA Security Rule Enough to Protect Electronic Personal Health Information (PHI) in the Cyber Age?'' *supra* note 207; *see also* Adam Wright, et al., ''The Big Phish: Cyberattacks Against U.S. Healthcare Systems,'' Journal of General Internal Medicine, Volume 31, p. 1115–1118 (May 13, 2016), *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5023604/.*

[972] *See* Thomas Clifford, ''Provider Liability and Medical Identity Theft: Can I Get Your (Insurance) Number?,'' Northwestern Journal of Law & Social Policy, Volume 12, p. 45 (2016), *https://scholarlycommons.law.northwestern.edu/njlsp/vol12/iss1/2/.*

[973] *Id.*

[974] *Id.*

[975] *See* ''Assessing resilience of hospitals to cyberattack,'' *supra* note 130; *see also* Ashley Carman, '' 'MEDJACK' tactic allows cyber criminals to enter healthcare networks undetected,'' SC Media (June 4, 2015) (''Medjack'' means a medical device hijack that attackers use to exploit outdated and unpatched medical devices), *https://www.scmagazine.com/news/medjack-tactic-allows-cyber-criminals-to-enter-healthcare-networks-undetected.*

[976] *See* ''New Dangers in the New World: Cyber Attacks in the Healthcare Industry,'' *supra* note 135.

[977] *See* Steven Ades, et al., ''Cancer Care in the Wake of a Cyberattack: How to Prepare and What to Expect,'' JCO Oncology Practice, Volume 18, p. 23–24 (Aug. 2, 2021), *https://pubmed.ncbi.nlm.nih.gov/34339260/.*

[978] *See* ''Assessing resilience of hospitals to cyberattack,'' *supra* note 130.

[979] *See* Mohammed Alkinoon, et al., ''Measuring Health Care Data Breaches,'' Information Security Applications, Volume 13009, p. 265–277 (Aug. 11, 2021), *https://dl.acm.org/doi/10.1007/978-3-030-89432-0_22.*

[980] *See* ''The Big Phish: Cyberattacks Against U.S. Healthcare Systems,'' *supra* note 971, p. 1115–1118.

[981] *See* ''Health Records Database and Inherent Security Concerns: A Review of the Literature,'' *supra* note 177.

withhold information from health care practitioners, ultimately compromising the decision-making capacity of their health care provider to administer the best quality of care.[982] Decreasing the number and scope of health care breaches would reduce the harms of such breaches and would be a significant benefit of the proposals in the NPRM.

5. Comparison of Benefits and Costs

Key inputs to the estimation of costs of this proposed rule include the numbers of regulated entities and health plan sponsors. The Department has not previously quantified the costs of Security Rule compliance for health plan sponsors because the existing requirements are for plan documents to require such sponsors to implement administrative, physical, and technical safeguards, but not necessarily to comply with the specific requirements of the Security Rule. Therefore, the proposed requirement to comply with the proposed changes to the Security Rule, along with the number of affected plan sponsors (approximately 740,000), results in a significant increase in overall cost estimates compared to the existing rule. The benefits of improved security for ePHI accrue to individuals, regulated entities, and health plan sponsors and are significant. The Department has discussed the benefits above.

The Department seeks to reduce the risk and mitigate the effects of breaches of ePHI and related information systems through the proposals included in this NPRM. Because the frequency and magnitude of cybersecurity events are inherently difficult to predict, we chose to conduct a break-even analysis in lieu of a cost savings analysis. The Department solicits comments with any information and data on the incidence and negative consequences of cybersecurity breaches.

The Department examined two different data points: the annual number of individuals affected by health care breaches, and the annual number of large breaches. Additionally, the Department considered a high and a low baseline based on the number of breaches and affected individuals per year. The Department calculated the high baseline as the average of the three highest values in the 6 years of available data (2018 to 2023, shown in table 8), and the low baseline as the average of the three lowest values.

TABLE 8—DATA ON BREACHES OF ePHI

Breach years	Affected individuals for large breaches [a]	Cost [b] per record [983]
2018	12,493,549	$488
2019	38,732,966	504
2020	37,641,403	476
2021	37,182,558	502
2022	41,747,613	477
2023	113,173,613	463
	Number of large breaches (500+ individuals)	Cost per breach
2018	302	12,012,809
2019	408	7,582,508
2020	656	8,273,537
2021	609	10,241,897
2022	626	10,468,138
2023	725	10,930,000

[a] The numbers of affected individuals and numbers of large breaches are contained in the Reports to Congress on Breaches of Unsecured Protected Health Information for years 2018–2022, *https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/reports-congress/index.html.* Data for 2023 is contained in OCR's breach portal, ''Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,'' Office for Civil Rights, U.S. Department of Health and Human Services, *https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.*

[b] The cost per record and cost per breach are based on estimates for health care breaches from the annual IBM Security and Ponemon Institute Costs of a Data Breach Reports for years 2018–2023. *See* ''Cost of a Data Breach Report 2023,'' IBM Security, p. 10, 13 (July 24, 2023), *available at https://www.ibm.com/reports/data-breach.* Because only general breach costs were available for the 2020–2023 period, the Department adjusted those by multiplying them by the average of the ratios of health care-specific to overall breach costs for the years for which both data points were available (2018, $408/$148 and 2019, $429/$150). All dollar values were converted to 2023 dollars using the seasonally adjusted GDP Implicit Price Deflator, *https://fred.stlouisfed.org/series/GDPDEF/.*

The high baseline used 669 breaches and a total of 71 million individuals affected, and the low baseline used 440 breaches and 29 million individuals affected.[984] The high baseline represents years with higher incidence of breaches, whereas the low baseline represents years with lower incidence.

For each data point, the Department calculated the number of breaches or affected individuals by which the affected universe would have to decrease for the proposed rule to fully offset the annualized costs of regulated entities.[985] Table 9 and the discussion that follows analyses the costs and cost savings based on the number of individuals affected by breaches in a year and the cost per individual's ePHI or medical record.

[982] *Id.; see also* Victoria Kisekka, et al., ''The Effectiveness of Health Care Information Technologies: Evaluation of Trust, Security Beliefs, and Privacy as Determinants of Health Care Outcomes,'' Journal of Medical Internet Research, Volume 20 (Apr. 11, 2018), *https://pubmed.ncbi.nlm.nih.gov/29643052/.*

[983] For this analysis, a record is the ePHI of one individual.

[984] *See* ''Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Year 2022,'' *supra* note 213, p. 9 (2023); ''December 2023 Healthcare Data Breach Report,'' *supra* note 960.

[985] The break-even calculations presented here only include regulated entities because breach data is not available for health plan sponsors. Including sponsors and assuming they have the same rate of breaches would result in a similar break-even point in terms of percent decrease from baseline.

TABLE 9—BREAK-EVEN THRESHOLDS BY NUMBER OF AFFECTED INDIVIDUALS

Baseline	Affected individuals	Regulated entities NPRM costs	Unit cost (per individual record)	Break-even threshold (NPRM cost ÷ unit cost)	Percent decrease (threshold ÷ affected) × 100
High	64,551,397	$2,251,258,305	$498	4,521,423	7
Low	29,006,854				16.4

The analysis in table 9 suggests that this NPRM would break even (cost savings would match monetized costs incurred) if the number of affected individuals is reduced by approximately 4.5 million. In years with a high incidence of breaches, this would be a reduction of approximately 7 percent, and in low-incidence years this would be a decrease of 16.4 percent. Thus, if the proposed changes in the NPRM reduce the number of affected individuals by 7 to 16 percent, the rule would pay for itself. Alternatively, the same cost savings may be achieved by lowering the cost per affected individual's ePHI by 7 percent ($35) and 16 percent ($82), respectively.

Table 10 analyzes the potential cost savings for regulated entities based on the annual number of large breaches of ePHI and the cost per breach, as shown below.

TABLE 10—BREAK-EVEN THRESHOLDS BY NUMBER OF LARGE BREACHES

Baseline	Breaches	NPRM cost for regulated entities	Unit cost (per breach)	Break-even threshold (NPRM cost ÷ unit cost)	Percent decrease (threshold ÷ breaches) × 100
High	669	$2,251,258,305	$11,136,982	202	30.1
Low	440				58.9

In table 10, the Department assumes that the average cost per breach in industry reports ($11.1 million, calculated as the average of the three highest values in table 9, adjusted for inflation) refers to large breaches of ePHI . The analysis in table 10 suggests that the NPRM would break even if the annual number of large breaches is reduced by approximately 202. In high-incidence years, this would be a reduction of approximately 30 percent, and in low-incidence years, this would be a decrease of 59 percent. Alternatively, the same cost savings may be achieved by lowering the cost per breach by 30 percent ($3.4 million) and 9 percent ($6.6 million), respectively.

B. Regulatory Alternatives to the Proposed Rule

The Department welcomes public comment on any benefits or drawbacks of the following alternatives it considered, but did not propose, while developing this proposed rule. We also request comment on whether the Department should reconsider any of the alternatives considered, and if so, why.

No Changes to the Security Rule

We considered not proposing revisions to the Security Rule. However, the Department believes that not revising the Security Rule would result in continued increases in both the number and size of breaches. Such increases would result in an exponential increase in costs as shown in table 8 above. If the modifications to the Security Rule result in even modest improvements to the security of ePHI, the reduction in the number and/or size of breaches would reduce the overall costs associated with breaches, including the costs of mitigating harm resulting from such breaches.

Email Security

The Department considered proposing a separate standard for regulated entities to secure email transmissions. In the Department's Cybersecurity Performance Goals,[986] the Department identifies email security as an essential goal for reducing risk from common email-based threats such as email spoofing, phishing, and fraud. Therein, the Department points to basic email protection controls identified in the Health Industry Cybersecurity Practices, such as spam/virus checking and real-time deny lists, as well as strategies that may be deployed across small, medium, and large organizations, including MFA for email access, email encryption, workforce education, and advance tooling (*e.g.,* URL click protection via analytics, attachment sandboxing).[987]

The Department is aware of the threat that email poses to the information systems of regulated entities and to the confidentiality, integrity, and availability of ePHI.[988] However, the Department believes that it is important that the Security Rule remain technology-neutral and that the security measures we propose in this NPRM apply to a regulated entity's information systems broadly, including email programs. For example, in this NPRM, the Department proposes to require regulated entities to encrypt all ePHI at rest and in transit and proposes a transmission security standard in which regulated entities would be required to deploy technical controls to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.[989] Therefore, the Department believes it is unnecessary to promulgate a separate standard for email security. Because the other technical controls, such as encryption and MFA, are already incorporated into the requirements that would protect relevant electronic information systems, the Department believes that adopting a separate secure email standard would duplicate costs without creating a net benefit.

[986] ''Cybersecurity Performance Goals,'' *supra* note 18.

[987] *Id.*

[988] According to the 2021 Verizon Data Breach Investigations Report, ''phishing was 'present in 36% of breaches (up from 25% last year);' [and] 23% of malware was delivered through email.'' *See* ''Technical Volume 2: Cybersecurity Practices for Medium and Large Healthcare Organizations,'' Cybersecurity Practice #1: Email Protection Systems, HHS Healthcare & Public Health Sector Coordinating Council, p. 13 (2023), *https://405d.hhs.gov/Documents/tech-vol2-508.pdf* (citing a 2021 Verizon Data Breach Investigations Report).

[989] *See* proposed 45 CFR 164.312(b)(2) and (g).

Additionally, the Department considered whether to heighten the existing expectation [990] for regulated entities to inform individuals before transmitting ePHI to the individual via unencrypted email in response to a request for access under 45 CFR 164.524 by this means. We considered whether to require such notification for different types of requests, such as different categories of PHI (*e.g.,* billing, lab results, etc.), determining whether the individual had already received such notice, or providing notification upon each disclosure. Instead, the Department has proposed to clarify that notification must be provided for each request made by the individual under the individual right of access at 45 CFR 164.524 for their ePHI to be transmitted via unsecure email. We believe that requiring a regulated entity to determine whether the individual had already received such notification would be more burdensome than incorporating the notification into the access request process, and instead, have proposed. We estimate that this could increase burdens for providing access via unsecure means by approximately one minute per request of this type. We lack data to estimate the number of requests for access via unsecure means.

Small and Rural Health Care Providers

Consistent with the requirement that the Secretary adopt security standards that take into account the needs and capabilities of small health care providers and rural health care providers,[991] the Department considered excepting small and rural health care providers from the requirement to perform penetration testing at proposed 45 CFR 164.308(h)(2)(iii) to lower anticipated costs of the rule for such providers. The Department estimates that approximately 90 percent of providers are small (based on revenue). Thus, the estimated cost reduction from this exemption (as compared to the proposed requirement for all regulated entities), would be approximately $266,389,139 [822,600 × .9 × 3 hours × $119.94 wage of an information security analyst] annually. While the Department is aware of the cost implications of this requirement for small and rural health care providers, we also believe that penetration testing is a critical component of managing vulnerability to cyberthreats across the health care sector. Additionally, we believe that setting different requirements for cybersecurity for small and rural health care providers would lead such health care providers to believe that they can limit their investment in cybersecurity. Given that a significant amount of health care is provided by small and rural health care providers, limiting their investment in cybersecurity would create a sizable gap in security protections. Such a gap has the potential to increase such providers' attractiveness to cybercriminals.

The Department also considered proposing to permit small and rural health care providers to adopt alternate compensating controls, in lieu of the specified implementation specifications, to meet certain standards. After careful consideration, the Department concluded that it potentially could be just as costly to identify and adopt compensating controls that are reasonable and appropriate for small and rural health care practices. Small and rural health care providers would likely need to either hire personnel or contract with cybersecurity experts to identify potential compensating controls that would meet the relevant standard and provide implementation support. Accordingly, the Department declines to put forward such proposals at this time.

The Federal Information Security Modernization Act

The Department considered the requirements of the Federal Information Security Modernization Act (FISMA) [992] and whether compliance with FISMA by Federal agencies that are also regulated entities would be comparable to meeting the proposals in this NPRM. FISMA requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.[993] After careful consideration, the Department does not believe that a regulated entity's compliance with FISMA would necessarily ensure compliance with all applicable proposed requirements in this NPRM because FISMA's requirements and the Security Rule's requirements are designed to serve different purposes. FISMA primarily focuses on securing Federal information systems, while the Security Rule applies specifically to ePHI. This NPRM contains specific proposed requirements, not found in FISMA, which are tailored to ensure the confidentiality, integrity, and availability of ePHI. Therefore, although the Department believes that FISMA requirements are consistent with those in the Security Rule and the proposals in this NPRM, we decline to propose that compliance with FISMA requirements would be a comparable alternative to compliance with the proposals in this NPRM. Instead, we believe that FISMA requirements complement the Security Rule and the proposed requirements and will facilitate the ability of regulated entities that are also subject to FISMA to fulfill their compliance with the HIPAA Rules.

Modifications to the Definition of ''Information System''

The Department considered proposing additional modifications to the definition of ''information system.'' The Security Rule currently defines the term ''information system'' as an interconnected set of information resources under the same direct management control that shares common functionality and includes hardware, software, information, data, applications, communications, and people.[994] This definition is based on the definition of ''general support system'' or ''system'' in the appendix to the 1996 version of OMB Circular A–130, Security of Federal Automated Information Systems.[995] We considered proposing to remove the phrase ''under the same direct management control'' as a potential way to clarify the application of the definition to cloud-based computing. Cloud computing applications play an important role in health care today. For example, many health care providers have implemented cloud-based electronic health records (EHRs) and practice management systems. These applications are used to create, receive, maintain, and transmit ePHI, and as such, should be included as components of a covered entity's relevant electronic information system, a term which is based upon the term ''information system.'' After careful consideration, we have decided to retain the phrase ''under the same direct

[990] *See* ''Individuals' Right under HIPAA to Access their Health Information 45 CFR 164.524,'' What is the liability of a covered entity in responding to an individual's access request to send the individual's PHI to a third party?, Office for Civil Rights, U.S. Department of Health and Human Services, *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.*

[991] 42 U.S.C. 1320d–2(d)(1)(A)(v).

[992] Public Law 113–283 (Dec. 18, 2014) (codified at 44 U.S.C. 3551 *et seq.*).

[993] *Id.*

[994] 45 CFR 164.304 (definition of ''Information system'').

[995] ''Managing Information as a Strategic Resource,'' Circular No. A–130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, Office of Management and Budget, Executive Office of the President (Feb. 8, 1996), *https://georgewbush-whitehouse.archives.gov/omb/circulars/a130/a130.html.*

management control'' and instead clarify in the preamble how the definition of ''information system'' applies in cloud computing environments. The Department also requests comment on the definition of ''information system'' and the extent of control a regulated entity has with respect to applications in cloud computing environments.

We also considered proposing to adopt the definition of ''information system'' in the Paperwork Reduction Act of 1995 (PRA) and the current operative version of OMB Circular A–130.[996] The PRA and OMB Circular A–130 define ''information system'' as ''a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.'' The Department declined to adopt this definition because the existing definition in the Security Rule based on the definition of ''system'' in the 1996 version of OMB Circular A–130 more accurately reflects the typical components of an information system and the full extent of resources that are addressed by the Security Rule. Additionally, the definition of ''information system'' in the PRA and current operative version of OMB Circular A–130 contains some terms that are defined by the HIPAA Rules and some that are not. As a result, adopting this definition would require the Department to propose definitions to such additional terms and to ensure that the manner in which the terms with existing definitions are used is consistent with those existing definitions, and we are concerned that such change could cause significant confusion for regulated entities.

We do not believe that either of the alternative definitions considered would have generated a quantifiable change in costs because the alternatives would be clarifications to existing requirements and would not have changed the scope of the Security Rule's applicability.

Exception From Multi-Factor Authentication (MFA) Requirement

The Department considered proposing an exception to the MFA authentication requirement that would permit regulated entities in the future to adopt other technologies, in lieu of MFA, that might offer a more secure method of authenticating user identity.[997] Based on discussions with cybersecurity experts, the Department believes that MFA is likely to remain the most secure method for authenticating user identity in future years. It may take different forms, but it will still, at its core, meet the definition of MFA proposed in this NPRM for the foreseeable future.[998]

While the Department acknowledges that technology will continue to evolve, we are unable to predict when and whether future technology will address identity verification and exceed the level of protection offered by MFA. This uncertainty renders us unable to articulate requirements specific enough to justify a purposeful exception. Because of the uncertainty surrounding new technologies, we are also unable to estimate costs of adopting this alternative. Our current view is that proposing and codifying such an exception would be premature, but we will revisit the proposed specific requirement for MFA, if adopted, and reconsider the need for an exception should a more secure technology emerge.

Transition for Business Associates and Group Health Plans

The Department considered requiring regulated entities to comply with all of the proposals in this NPRM by the compliance date, rather than proposing transition provisions for existing business associate agreements or other contractual arrangements. Had the Department taken that approach, we would have proposed that regulated entities update all existing business associate agreements by the proposed compliance date to comply with all applicable proposed requirements in this NPRM. While the Department believes that many of the proposals in this NPRM are consistent with the Security Rule as it currently exists, we are also concerned that too many regulated entities are not currently compliant with the Security Rule. Given the demonstrable increase in breaches, we believe that it is more important for regulated entities to first improve their cybersecurity posture by coming into compliance with all applicable proposed requirements in this NPRM, if adopted. Upon doing so, the Department anticipates that regulated entities will be better positioned to evaluate their contractual needs and to modify existing business associate agreements. For this reason, the Department has proposed the transition provisions in proposed 45 CFR 164.318. Not allowing for a transition period could have an opportunity cost whereby regulated entities spend their limited time revising business associate agreements instead of enhancing their cybersecurity posture. The Department believes that this could result in duplicative costs because some regulated entities may identify the need for additional changes to business associate agreements after they have fully evaluated their changed cybersecurity needs. The Department estimates that small regulated entities may be more likely to experience that outcome without a transition period, and thus the alternative of no transition period would cause a potential one-time increase in costs of $278,332,891 [(1,822,600 regulated entities × .9) × 1 hour × $169.68 lawyer hourly wage].

Relatedly, the Department considered proposing similar transition provisions for group health plans and plan sponsors that would provide these entities with additional time to update plan documents to align with new proposed requirements in this NPRM, if adopted. However, the Department believes that affected plans and plan sponsors would be able to complete any necessary updates by the proposed compliance date. The Department believes that updating plan documents is not as complex a task as evaluating potential new contractual needs to meet business associate obligations. Additionally, plan sponsors do not have Security Rule obligations independent of plan documents, and thus would not be obligated to implement the requirements proposed in this NPRM absent updates to the plan documents. The result of a transition period for updating plan documents would be merely to delay compliance with the changed Security Rule requirements, and therefore, delay improvements to their cybersecurity posture, not to reduce costs. Accordingly, we are not proposing such transition provisions in this NPRM.

C. Regulatory Flexibility Act—Small Entity Analysis

The Department has examined the economic implications of this proposed rule as required by the RFA. If a rule has a significant economic impact on a substantial number of small entities, the RFA requires agencies to analyze regulatory options that would reduce the economic effect of the rule on small entities. As discussed in greater detail below, this analysis concludes, and the Secretary proposes to certify, that the proposed rule, if finalized, would not

[996] Public Law 104–13, 109 Stat. 166 (May 22, 1995) (codified at 44 U.S.C. 3502(8)) (definition of ''information system''); *see also* ''Managing Information as a Strategic Resource,'' Circular No. A–130, Office of Management and Budget, Executive Office of the President, p. 31 (Jul. 28, 2016), (definition of ''information system'') *https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf.*

[997] Proposed 45 CFR 164.312(f)(2)(ii).

[998] 45 CFR 164.304 (proposed definition of ''Multi-factor authentication'').

result in a significant economic effect on a substantial number of small entities.

For purposes of the RFA, small entities include small businesses, nonprofit organizations, and small governmental jurisdictions. The Act defines ''small entities'' as (1) a proprietary firm meeting the size standards of the SBA, (2) a nonprofit organization that is not dominant in its field, and (3) a small government jurisdiction of less than 50,000 population. The Department has determined that roughly 90 percent or more of all health care providers meet the SBA size standard for a small business as shown in table 4 or are a nonprofit organization. Therefore, the Department estimates that there would be 740,348 small entities affected by the proposals in this proposed rule.[999] The SBA size standard for health care providers ranges between a maximum of $9 million and $47 million in annual receipts, depending upon the type of entity, as shown in table 4, above.[1000]

With respect to health insurers, the SBA size standard is a maximum of $47 million in annual receipts, and for pharmacy benefits and clearinghouses it is $45.5 million.[1001] While some insurers are classified as nonprofit, it is possible they are dominant in their market. For example, a number of Blue Cross/Blue Shield insurers are organized as nonprofit entities; and yet, they dominate the health insurance market in the States where they are licensed.[1002]

With respect to business associates, they provide a wide range of services for covered entities, including computer infrastructure, clearinghouse activities, leased office equipment, and professional services, such as legal, accounting, business planning, and marketing. The SBA size thresholds for these industries ranges from $15.5 million for lawyers to $47 million for clearinghouses.[1003]

For the reasons stated below, the Department does not expect that the cost of compliance would be significant for small entities. Nor does the Department expect that the cost of compliance would fall disproportionately on small entities. Although many of the regulated entities affected by the proposals in this proposed rule are small entities, they would not bear a disproportionate cost burden compared to the other entities subject to the rule. The projected total costs are discussed in detail in the RIA. The Department does not view this as a substantial burden because the result of the changes would be annualized costs per regulated entity of approximately $1,235 [= $2.3 billion[1004]/1,822,600 regulated entities]. The per-entity costs represent the costs per establishment. As a result, smaller entities' costs are lower because they have fewer establishments. Larger regulated entities (*i.e.,* firms) that have multiple facilities (*i.e.,* establishments) would experience higher costs than the average cost per establishment because each firm would need to apply the proposals to all of their establishments. In the context of the RFA, HHS generally considers an economic impact exceeding 3 percent of annual revenue to be significant, and 5 percent or more of the affected small entities within an identified industry to represent a substantial number.

More than 5 percent of the small covered entities listed under the NAICS codes in table 4 are one-establishment firms with fewer than five employees,[1005] so the analysis must determine how the effects of the quantified costs on one-establishment firms compare to their revenues. As explained above, the cost for a one-establishment firm is $1,235, so only small firms whose revenues are below $41,167 [=$1,235/0.03] would experience an effect exceeding 3 percent.

Among the NAICS codes for health care providers, the small firms with the lowest revenues are one-establishment HMO [Health Maintenance Organization] Medical Centers (NAICS 621491) with fewer than five employees, which had an estimated average yearly revenue in 2021 of $108,000. Residential Intellectual and Developmental Disability Facilities (NAICS 623210) had the second lowest revenues for one-establishment firms with fewer than five employees, with $180,000. Offices of Mental Health Practitioners (NAICS 621330) have the third lowest revenues for one-establishment firms with fewer than five employees, with $189,000. Thus, the Department believes that almost all regulated entities have annual revenues that exceed these amounts.

The Department acknowledges that there may be very small firms—namely firms without employees—whose revenues are below $41,167. We believe that such firms would comply with the regulation by purchasing services from software and web-hosting companies whose costs may increase as a result of the proposed changes. Such software and web-hosting companies would be business associates, and thus costs to them are already accounted for. We believe that, to the extent that these business associates decide to recover their minor cost increases by raising the prices of the services sold to non-employer firms, these incremental costs passed through to their small-firm customers would be negligible because they will be spread among many non-employer firms.

The Department has separately analyzed the effects of the NPRM on health plan sponsors and does not view the projected costs as a significant burden because the proposed changes would result in annualized costs per plan sponsor of approximately $6,133 [=$4,552,995,816/742,411 health plan sponsors]. The quantified impact of $6,133 per health plan sponsor would only apply to those sponsors whose annual revenue is $204,433 or less.[1006] The Department believes there are few, if any, group health plan sponsors with annual revenues below this amount because the average revenue of a U.S. business with 1–4 employees is $387,000[1007] and employers with 0–1 employees are unlikely to sponsor a group health plan.

Accordingly, the Department believes that this proposed rule, if adopted, would be unlikely to affect a substantial

[999] 740,348 = 822,609 covered entities × .90.

[1000] *See* ''Table of Small Business Size Standards,'' U.S. Small Business Administration (Mar. 17, 2023), *https://www.sba.gov/sites/sbagov/files/2023-06/Table%20of%20Size%20Standards_Effective%20March%2017%2C%202023%20%282%29.pdf.*

[1001] *Id.*

[1002] ''Market Share and Enrollment of Largest Three Insurers—Large Group Market,'' Kaiser Family Foundation (2019), *https://www.kff.org/other/state-indicator/market-share-and-enrollment-of-largest-three-insurers-large-group-market/?currentTimeframe=0&sortModel=%7B%22colId%22:%22Location%22,%22sort%22:%22asc%22%7D.*

[1003] *See* ''Table of Small Business Size Standards,'' *supra* note 1000.

[1004] This figure is rounded and represents annualized costs discounted at a 2 percent rate. The actual figure is $2,251,258,305.

[1005] SUSB 2017 reports average revenue per firm by employment size. The size categories begin with less than 5 employees followed by 5 to 10 employees, and so on, with the largest categories representing firms with 2,500 to 4,999 employees and 5,000 or more employees). ''2017 [Statistics of U.S. Businesses] Annual Data Tables by Establishment Industry,'' (May 2021), *https://www.census.gov/data/tables/2017/econ/susb/2017-susb-annual.html.* We inflated these revenues to 2021 dollars using the GDP deflator to estimate average revenues in each employment class in 2021 because that is the latest year for which data is reported. *See* ''2021 [Statistics of U.S. Businesses] SUSB Annual Data Tables by Establishment Industry,'' *supra* note 947. We then concluded that more than 5 percent of the firms whose revenues fall below the SBA thresholds (see table 4) belong to the ''fewer than 5 employees'' category and operate a single establishment.

[1006] $6,133 is 3 percent of $204,433.

[1007] ''Average Small Business Revenue: What To Know,'' Fora Financial (Jan. 11, 2023), *https://www.forafinancial.com/blog/small-business/average-small-business-revenue/.*

number of small entities that meet the RFA threshold. Thus, this analysis concludes, and the Secretary proposes to certify, that the NPRM would not result in a significant economic effect on a substantial number of small entities.

HIPAA requires the Department to consider the needs and capabilities of small and rural health care providers.[1008] As we explained in our 2003 analysis of the effect of the Security Rule on small and rural health care providers, the scalability provisions preclude the need to precisely define those categories.[1009] We have long considered the effect of our rules on small businesses in the Small Entity Analysis discussed above. However, because of the breadth of changes proposed in this NPRM, the Department has considered more closely how it would affect rural health care providers. There are approximately 2,000 rural hospitals,[1010] comprising nearly 30 percent of all hospitals [= 2,057/7,465],[1011] and the Department estimates approximately 7 to 8 percent of all health care providers operate in rural areas (counties or micropolitan areas with fewer than 50,000 inhabitants). See Regulated Entities Affected in Section V.A.2. Baseline Conditions, above.

Because rural health care providers are more likely to be small businesses, they would be affected in a manner similar to small entities, as demonstrated in the Small Entity Analysis above. Likewise, to the extent that Tribal health care providers are in rural areas, which many are,[1012] our analysis of the effects on rural health care providers generally also applies. However, Tribal health providers have the benefit of access to centralized supportive services for health IT and EHR adoption, which other rural providers may lack.[1013] A primary barrier to both adoption of health information technology (health IT) and deployment of cybersecurity safeguards in rural communities is limited access to high-speed internet. Rural health care providers, such as hospitals, have adopted EHRs at a lower rate than non-rural hospitals,[1014] and thus may also have fewer electronic information systems that are subject to the Security Rule requirements, which could ease some burdens of compliance. However, as EHR adoption has increased in rural hospitals,[1015] so too have the risks of cybersecurity attacks.[1016] Rural health care providers are more likely to have limited resources to update legacy information technology (IT) systems, implement new or changed regulatory requirements, and respond to large breaches. Additionally, the health IT workforce is more limited in rural areas, which may affect the ability of rural health care providers to access in-person technical assistance. Because most rural hospitals are ''located more than 35 miles from another hospital,'' responding to cyberattacks may be more challenging.[1017] We request comment on the burdens these proposals would impose on rural health care providers, including rural hospitals.

Rural health care providers and other regulated entities can avail themselves of grants and incentives to improve broadband access and adoption of health IT.[1018] For cybersecurity in particular, the White House, in partnership with private companies, announced the availability of direct assistance to rural health care providers on cybersecurity in the form of grants, discounts, and technical advice.[1019] Additionally, CISA has compiled a list of free services and tools available to regulated entities from private and public sector entities. CISA also has published, in partnership with the Joint Cyber Defense Collaborative, a list of cybersecurity resources especially focused on high-risk communities.[1020] And the Advanced Research Projects Agency for Health announced plans to invest $50 million to develop an autonomous solution for addressing cyberthreats to assist hospitals in defending their information systems.[1021]

Cybersecurity is as essential for small and rural health care providers and their business associates, as it is for large and urban regulated entities. The seamless flow of data and increased connectivity means that threats to one health care provider do not affect only that one health care provider, regardless of size or location. The effects on patient care may be greater in rural environments where fewer alternatives exist if care is delayed or denied as a result of a cyberattack or malfunction.[1022] As discussed in the preamble, the factors described at 45 CFR 164.306(b)(2) provide the flexibility for small and rural providers, in particular, to adopt security measures that are reasonable and appropriate for their circumstances.

D. Executive Order 13132—Federalism

As required by E.O. 13132 on Federalism,[1023] the Department has examined the provisions in the proposed regulation for their effects on the relationship between the Federal Government and the States. E.O. 13132 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent final rule) that imposes substantial direct requirement costs on State and local governments, preempts State law, or otherwise has federalism implications. In the Department's view, the proposed rule would not have any federalism implications.

The federalism implications of the Security Rule were also assessed as required by E.O. 13132 and published as part of the preambles to the final rules on February 20, 2003 [1024] and January

[1008] 42 U.S.C. 1320d–2(d).

[1009] *See* 68 FR 8334, 8341 (Feb. 20, 2003).

[1010] *See* ''Fact Sheet: Biden-Harris Administration Bolsters Protections for Americans' Access to Healthcare Through Strengthening Cybersecurity,'' *supra* note 306. *See also* table 4 above, SBA size threshold for hospitals.

[1011] *See* ''2021 [Statistics of U.S. Businesses] SUSB Annual Data Tables by Establishment Industry,'' *supra* note 947 (count of hospitals).

[1012] The Indian Health Service funds a ''network of over 600 hospitals, clinics, and health stations on or near Indian reservations in service areas that are rural, isolated, and underserved.'' ''Justification of Estimates for Appropriations Committees, Fiscal Year 2025'' Indian Health Service, U.S. Department of Health and Human Services, p. CJ–39 (Mar. 5, 2024).

[1013] *See id.* at p. CJ–63–75.

[1014] *See* ''Telehealth and Health Information Technology in Rural Healthcare,'' Rural Health Information Hub, *https://www.ruralhealthinfo.org/topics/telehealth-health-it#challenges-for-rural-communities.*

[1015] *See* ''Percent of Hospitals, By Type, that Possess Certified Health IT,'' *supra* note 298.

[1016] Kat Jercich, ''Rural hospitals are more vulnerable to cyberattacks—here's how they can protect themselves,'' *supra* note 295.

[1017] *See* ''Fact Sheet: Biden-Harris Administration Bolsters Protections for Americans' Access to Healthcare Through Strengthening Cybersecurity,'' *supra* note 306.

[1018] Hannah Neprash, et al., ''What happens to rural hospitals during a ransomware attack? Evidence from Medicare data,'' The Journal of Rural Health (Mar. 17, 2024), *https://pubmed.ncbi.nlm.nih.gov/38494590/.* For information about grants and incentives available for improving broadband access and adoption of health IT, *see, e.g.,* ''Funding Programs,'' BroadbandUSA, National Telecommunications and Information Administration, U.S. Department of Commerce, *https://broadbandusa.ntia.doc.gov/funding-programs;* ''Rural Health Care Program,'' Federal Communications Commission, *https://www.fcc.gov/general/rural-health-care-program.*

[1019] *See* ''Fact Sheet: Biden-Harris Administration Bolsters Protections for Americans' Access to Healthcare Through Strengthening Cybersecurity,'' *supra* note 306.

[1020] *See, e.g.,* ''Free Cybersecurity Services and Tools,'' *supra* note 313; ''Cybersecurity Resources for High-Risk Communities,'' *supra* note 313.

[1021] *See* ''Fact Sheet: Biden-Harris Administration Bolsters Protections for Americans' Access to Healthcare Through Strengthening Cybersecurity,'' *supra* note 306; *see also* ''UPGRADE, Universal Patching and Remediation for Autonomous Defense,'' Advanced Research Projects Agency for Health (May 20, 2024), *https://arpa-h.gov/research-and-funding/programs/upgrade.*

[1022] ''What happens to rural hospitals during a ransomware attack? Evidence from Medicare data,'' *supra* note 1018.

[1023] 64 FR 43255 (Aug. 4, 1999).

[1024] 68 FR 8334, 8373 (Feb. 20, 2003).

25, 2013.[1025] Regarding preemption, HIPAA dictates the relationship between State law and HIPAA regulatory requirements.[1026] The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act) provides that the HIPAA preemption provisions shall apply to the HITECH Act provisions and requirements.[1027] As explained by the House report that accompanied the American Recovery and Reinvestment Act of 2009, the HITECH Act would not only apply HIPAA's preemption provisions to the HITECH Act requirements, but it would also ''preserve the HIPAA privacy and security standards to the extent that they are consistent with'' the HITECH Act.[1028]

A requirement, standard, or implementation specification adopted in accordance with HIPAA and the HIPAA Rules supersedes any contrary provision of State law, subject to certain exceptions.[1029] Specifically, State law would be preempted under the Security Rule only when (1) a regulated entity finds it impossible to comply with both State and Federal requirements; or (2) the provision of State law stands as an obstacle to accomplishing and executing the purposes and objectives of the Administrative Simplification provisions or the HITECH Act.[1030] Although a few States (*e.g.,* California and New York) have promulgated or are in the process of promulgating regulations pertaining to cybersecurity in health care that may be more stringent than the Security Rule, the Department believes that a regulated entity could comply with both sets of requirements by adhering to the more stringent standard. Thus, in such cases, the State law would not be an obstacle to the accomplishment and execution of HIPAA or the HITECH Act.

The proposed modifications to the Security Rule would further the Congressional intent to improve the Medicare and Medicaid programs by the development of health information systems that are private and secure. The Department's proposals promote the safety, efficiency, and effectiveness of the health care system by refining the security standards established by Congress and implemented in the 2003 and 2013 Final Rules. The statute contemplated that the security measures adopted by all regulated entities, including State and local governments, would evolve over time in accordance with the security risks they face, and the NPRM proposals are in the nature of enhancing these existing requirements. Thus, the Department does not believe that the rule would impose substantial direct compliance costs on State and local governments that are not required by statute.

The Department anticipates that the most significant direct costs on State and local governments would be for conducting a Security Rule compliance audit; notifying covered entities or business associates, as applicable, upon activation of a contingency plan; notifying covered entities of changes or termination of workforce members' access to ePHI; deploying MFA; removing extraneous software; and penetration testing; providing or obtaining verification of business associates' compliance with technical safeguards; updating health plan documents; updating policies and procedures; and updating workforce training. However, the costs involved can be attributed to the statutory requirements of the Administrative Simplification provisions of HIPAA and would be similar in kind to those borne by non-government-operated regulated entities, which the proposed RIA above addresses in detail.

In considering the principles in and requirements of E.O. 13132, the Department believes that these proposed modifications to the Security Rule would not significantly affect the rights, roles, and responsibilities of the States and requests comment on this analysis.

E. Assessment of Federal Regulation and Policies on Families

Section 654 of the Treasury and General Government Appropriations Act of 1999[1031] requires Federal departments and agencies to determine whether a proposed policy or regulation could affect family well-being. If the determination is affirmative, then the Department or agency must prepare an impact assessment to address criteria specified in the law. This proposed rule is expected to strengthen family well-being because it would ensure a baseline of security measures for individuals' PHI, and medical information and decisions based on that information are at the heart of family decision making. If finalized, the provisions in this proposed rule may be carried out only by the Federal Government because it would modify Federal law on cybersecurity in health care, ensuring that American families have confidence that the privacy of their PHI is secured by consistent safeguards, regardless of the State where they are located when health care is provided. Such health care privacy and is vital for individuals who seek or access health care.

F. Paperwork Reduction Act of 1995

Under the PRA,[1032] agencies are required to submit to OMB for review and approval any reporting or recordkeeping requirements inherent in a proposed or final rule and are required to publish such proposed requirements for public comment. To fairly evaluate whether an information collection should be approved by the OMB, section 3506(c)(2)(A) of the PRA requires that the Department solicit comment on the following issues:

1. Whether the information collection is necessary and useful to carry out the proper functions of the agency.

2. The accuracy of the agency's estimate of the information collection burden.

3. The quality, utility, and clarity of the information to be collected.

4. Recommendations to minimize the information collection burden on the affected public, including automated collection techniques.

The PRA requires consideration of the time, effort, and financial resources necessary to meet the information collection requirements referenced in this section. The Department solicits public comments on its assumptions and burden estimates in this NPRM as summarized below.

In this RIA, the Department proposes to revise certain information collection requirements associated with this NPRM and, as such, would revise the information collection last prepared in 2024 and approved under OMB control #0945–0003.[1033] The proposed revisions to the information collection describe all new and adjusted information

[1025] 78 FR 5566, 5686 (Jan. 25, 2013).

[1026] 42 U.S.C. 1320d–7.

[1027] Sec. 13421(a) of the HITECH Act; *see also* 45 CFR part 160, subpart B.

[1028] *See* ''MAKING SUPPLEMENTAL APPROPRIATIONS FOR JOB PRESERVATION AND CREATION, INFRASTRUCTURE INVESTMENT, ENERGY EFFICIENCY AND SCIENCE, ASSISTANCE TO THE UNEMPLOYED, AND STATE AND LOCAL FISCAL STABILIZATION, FOR THE FISCAL YEAR ENDING SEPTEMBER 30, 2009, AND FOR OTHER PURPOSES,'' Conf. Report to Accompany H.R. 1, p. 502 (Feb. 12, 2009).

[1029] 42 U.S.C. 1320d–7(a); 45 CFR 160.203.

[1030] *See* 45 CFR 160.202 (definition of ''Contrary''). Preemption also applies if the provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives and purposes of sec. 264 of HIPAA. Sec. 264 of HIPAA contains the provisions pertaining to the privacy of individually identifiable health information.

[1031] Public Law 105–277, 112 Stat. 2681–528 (Oct. 21, 1998) (codified at 5 U.S.C. 601 note).

[1032] Public Law 104–13, 109 Stat. 163 (May 22, 1995) (codified at 44 U.S.C. 101 note).

[1033] ''View ICR,'' *supra* note 940.

collection requirements for regulated entities pursuant to the implementing regulation for HIPAA at 45 CFR parts 160 and 164, the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules (''HIPAA Rules'').

The estimated annual labor burden presented by the regulatory modifications is 77,067,552 burden hours at a first-year cost of $9,314,106,174. These figures, respectively, represent the sum of 37,781,637 new burden hours at a cost of $4,655,324,954 for compliance by regulated entities and 39,285,915 new burden hours at a cost of $4,658,781,219 for compliance by health plan sponsors.

The overall total burden for respondents to comply with the information collection requirements of all of the HIPAA Privacy, Security, and Breach Notification Rules, including new burdens presented by proposed program changes, is estimated to be 925,144,023 burden hours at a cost of $109,085,104,674, plus $163,499,411 in capital costs for a total estimated annual burden of $109,248,604,085, after the effective date of the final rule. This estimate is based on a total of 1,202,562,864 responses for a total of 2,565,011 respondents. The total burden for the HIPAA Rules, including the changes proposed in this NPRM, would result in a decrease of 28,838,213 burden hours and a cost increase of $1,911,898,144, in comparison to the baseline in the ICR associated with the 2024 Privacy Rule to Support Reproductive Health Care Privacy.[1034] This is the result of multiples changes, such as decreasing burden hours for some existing requirements, increasing the estimated number of covered entities, adding new Security Rule requirements, and expanding the pool of respondents for the Security Rule by adding requirements for health plan sponsors.

Details describing the burden analysis for the proposals associated with this RIA are presented below and explained further in the ICR associated with the NPRM.

1. Explanation of Estimated Annualized Burden Hours

Below is a summary of the significant program changes and adjustments proposed since the approved 2024 ICR; because the ICR addresses regulatory burdens associated with the full suite of HIPAA Rules, the changes and adjustments include updated data and estimates for some provisions of the HIPAA Rules that are not affected by this proposed rule. These program changes and adjustments form the bases for the burden estimates presented in the ICR associated with this NPRM.

Adjusted Estimated Annual Burdens of Compliance

(1) Updating the number of covered entities.

(2) Updating hourly wage rates.

(3) Adjusting downward the number of estimated requests for an exception to Federal preemption of State law to the prior baseline of 1 request per year.

(4) Adjusting downward the estimated hourly burden for regulated entities to report security incidents (not breaches) from 20 hours per monthly report to 10 hours per monthly report.

(5) Updating the number of research disclosures.

New Burdens Resulting From Program Changes

In addition to the adjustments above, the Department proposes to add new annual estimated burdens as a result of program changes, as follows:

(1) A burden of 2 hours for each regulated entity to conduct a Security Rule compliance audit.

(2) A burden of 2 hours for each business associate (including each subcontractor) to provide verification of compliance with technical safeguards.

(3) A burden of .5 hours for each covered entity to obtain verification of business associates' compliance with technical safeguards.

(4) A burden of .083 hours for each business associate to obtain verification of subcontractors' compliance with technical safeguards.

(5) A burden of 1 hour for each regulated entity to provide notification to other regulated entities of workforce members' termination of access to ePHI.

(6) A burden of 1.5 hours for each regulated entity to deploy MFA.

(7) A burden of 4.5 hours for each regulated entity to perform network segmentation.

(8) A burden of .5 hours for approximately 76.56 percent of regulated entities to disable unused ports and remove extraneous software.

(9) A burden of 3 hours for each regulated entity to conduct penetration testing.

(10) A burden of .5 hours for each regulated entity to notify covered entities or business associates, as applicable, upon activation of a contingency plan.

(11) A burden of .5 hours for each insurer and third-party administrator to update health plan documents.

(12) A burden of 2 hours for each regulated entity to update the content of its cybersecurity awareness and Security Rule training program.

(13) A burden of 3.5 hours for each regulated entity to update its policies and procedures.

(14) A burden of 1 hour for each regulated entity to update business associate agreements.

(15) A burden of 52.92 hours for each health plan sponsor to modify safeguards for its relevant electronic information systems to meet Security Rule standards.

List of Subjects

45 CFR Part 160

Administrative practice and procedure, Computer technology, Electronic information system, Electronic transactions, Employer benefit plan, Group health plan, Health, Health care, Health facilities, Health insurance, Health professions, Health records, Hospitals, Investigations, Medicaid, Medical Research, Medicare, Penalties, Preemption, Privacy, Public health, Reporting and recordkeeping requirements, Security.

45 CFR Part 164

Administrative practice and procedure, Computer technology, Drug abuse, Electronic information system, Electronic transactions, Employer benefit plan, Group health plan, Health, Health care, Health facilities, Health insurance, Health professions, Health records, Hospitals, Medicaid, Medical research, Medicare, Privacy, Public health, Reporting and recordkeeping requirements, Security.

Proposed Rule

For the reasons stated in the preamble, the Department of Health and Human Services proposes to amend 45 CFR subtitle A, subchapter C, parts 160 and 164 as set forth below:

PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS

■ 1. The authority citation for part 160 continues to read as follows:

Authority: 42 U.S.C. 1302(a); 42 U.S.C. 1320d–1320d–9; sec. 264, Pub. L. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320d–2 (note)); 5 U.S.C. 552; secs. 13400–13424, Pub. L. 111–5, 123 Stat. 258–279; and sec. 1104 of Pub. L. 111–148, 124 Stat. 146–154.

■ 2. Amend § 160.103 by revising the definition of ''Electronic media'' to read as follows:

§ 160.103 Definitions.

* * * * *

Electronic media means:

(1) Electronic storage material on which data may be recorded, maintained, or processed. This includes, but is not limited to, hard drives,

[1034] *Id.*

removable media, magnetic tape, optical disk, and any other form of digital memory or storage.

(2) Transmission media used to exchange information already in electronic storage material. Transmission media includes, but is not limited to, the internet, extranet or intranet, leased lines, dial-up lines, private and public networks, and the physical movement of removable/transportable electronic storage material.

* * * * *

PART 164—SECURITY AND PRIVACY

■ 1. The authority citation for part 164 continues to read as follows:

Authority: 42 U.S.C. 1302(a); 42 U.S.C. 1320d–1320d–9; sec. 264, Pub. L. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320d–2(note)); and secs. 13400–13424, Pub. L. 111–5, 123 Stat. 258–279.

■ 2. Revise and republish subpart C to read as follows:

Subpart C—Security Standards for the Protection of Electronic Protected Health Information

Sec.

164.302 Applicability.
164.304 Definitions.
164.306 Security standards: General rules.
164.308 Administrative safeguards.
164.310 Physical safeguards.
164.312 Technical safeguards.
164.314 Organizational requirements.
164.316 Documentation requirements.
164.318 Transition provisions.
164.320 Severability.
Appendix A to Subpart C of Part 164—Security Standards: Matrix

Authority: 42 U.S.C. 1320d–2 and 1320d–4; 42 U.S.C. 17931.

§ 164.302 Applicability.

A covered entity or business associate must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information of a covered entity.

§ 164.304 Definitions.

As used in this subpart, the following terms have the following meanings:

Access means the ability or the means necessary to read, write, modify, delete, transmit, or communicate data/information or otherwise use any component of an information system. (This definition applies to ''access'' as used in this subpart, not as used in subpart D or E of this part.)

Administrative safeguards are administrative actions and related policies and procedures to manage the selection, development, implementation, and maintenance (including updating and modifying) 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.

Authentication means the corroboration that a person or technology asset is the one they are claiming to be.

Availability means the property that data or information is accessible and useable upon demand by an authorized person or technology asset.

Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons, technology assets, or processes.

Deploy means to configure technology for use and implement such technology.

Electronic information system means interconnected set of electronic information resources under the same direct management control that shares common functionality. An electronic information system generally includes technology assets, such as hardware, software, electronic media, information, and data.

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Facility means the physical premises and the interior and exterior of a building(s).

Implement means to put into effect and be in use, operational, and function as expected throughout the covered entity or business associate.

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. An information system generally includes hardware, software, information, data, communications, and people.

Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner.

Malicious software means software or firmware intended to perform an unauthorized action or activity that will have adverse impact on an electronic information system and/or the confidentiality, integrity, or availability of electronic protected health information. Examples include but are not limited to viruses, worms, Trojan horses, spyware, and some forms of adware.

Multi-factor authentication means authentication of the user's identity through verification of at least two of the following three categories:

(1) Information known by the user, including but not limited to a password or personal identification number (PIN).

(2) Item possessed by the user, including but not limited to a token or a smart identification card.

(3) Personal characteristic of the user, including but not limited to fingerprint, facial recognition, gait, typing cadence, or other biometric or behavioral characteristics.

Password means confidential authentication information composed of a string of characters, such as letters, numbers, spaces, and other symbols.

Physical safeguards are physical measures and related policies and procedures to protect a covered entity's or business associate's relevant electronic information systems, and related facilities and equipment, from natural and environmental hazards and unauthorized intrusion.

Relevant electronic information system means an electronic information system that creates, receives, maintains, or transmits electronic protected health information or that otherwise affects the confidentiality, integrity, or availability of electronic protected health information.

Risk means the extent to which the confidentiality, integrity, or availability of electronic protected health information is threatened by a potential circumstance or event.

Security or *security measures* encompass all of the administrative, physical, and technical safeguards in or applied to an information system.

Security incident means any of the following:

(1) The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information in an information system.

(2) The attempted or successful unauthorized interference with system operations in an information system.

Technical controls means the technical mechanisms contained in the hardware, software, or firmware components of an electronic information system that are primarily implemented and executed by the electronic information system to protect the information system and data therein.

Technical safeguards means the technology, technical controls, and related policies and procedures governing the use of the technology that protects and controls access to electronic protected health information.

Technology asset means the components of an electronic information system, including but not

limited to hardware, software, electronic media, information, and data.

Threat means any circumstance or event with the potential to adversely affect the confidentiality, integrity, or availability of electronic protected health information.

User means a person with authorized access.

Vulnerability means a flaw or weakness in an information system, information system security procedures, design, implementation, or technical controls that could be intentionally exploited or accidentally triggered by a threat.

Workstation means an electronic computing device and electronic media stored in its immediate environment. Workstation includes but is not limited to the following types of devices: a server, desktop computer, laptop computer, virtual device, and mobile device such as a smart phone or tablet.

§ 164.306 Security standards: General rules.

(a) *General requirements.* Each covered entity and business associate must do the following with respect to all electronic protected health information it creates, receives, maintains, or transmits:

(1) Ensure the confidentiality, integrity, and availability of the electronic protected health information.

(2) Protect against any reasonably anticipated threats or hazards to the confidentiality, integrity, or availability of the electronic protected health information.

(3) Protect against any reasonably anticipated uses or disclosures of the electronic protected health information that are not permitted or required under subpart E of this part.

(4) Ensure compliance by its workforce with this subpart and all administrative, physical, and technical safeguards implemented in accordance with this subpart.

(b) *Flexibility of approach.* (1) Covered entities and business associates may use any reasonable and appropriate security measures that allow the covered entity or business associate to implement the standards and implementation specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity or business associate must take into account all of the following factors:

(i) The size, complexity, and capabilities of the covered entity or business associate.

(ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.

(iii) The costs of security measures.

(iv) The probability and criticality of potential risks to electronic protected health information.

(v) The effectiveness of the security measure in supporting the resiliency of the covered entity or business associate.

(c) *Standards and implementation specifications.* A covered entity or business associate must comply with the applicable standards, including their implementation specifications, as provided in this subpart.

§ 164.308 Administrative safeguards.

(a) A covered entity or business associate must, in accordance with §§ 164.306 and 164.316, implement all of the following administrative safeguards to protect the confidentiality, integrity, and availability of all electronic protected health information that it creates, receives, maintains, or transmits:

(1) *Standard: Technology asset inventory*—(i) *General.* Conduct and maintain an accurate and thorough written inventory and a network map of the covered entity's or business associate's electronic information systems and all technology assets that may affect the confidentiality, integrity, or availability of electronic protected health information.

(ii) *Implementation specifications*—(A) *Inventory.* Develop a written inventory of the covered entity's or business associate's technology assets that contains the identification, version, person accountable, and location of each technology asset.

(B) *Network map.* Develop a network map that illustrates the movement of electronic protected health information throughout the covered entity's or business associate's electronic information systems, including but not limited to how electronic protected health information enters and exits such information systems, and is accessed from outside of such information systems.

(C) *Maintenance.* Review and update the written inventory of technology assets required by paragraph (a)(1)(ii)(A) of this section and the network map required by paragraph (a)(1)(ii)(B) of this section in the following circumstances:

(*1*) On an ongoing basis, but at least once every 12 months.

(*2*) When there is a change in the covered entity's or business associate's environment or operations that may affect electronic protected health information, including but not limited to the adoption of new technology assets; the upgrading, updating, or patching of technology assets; newly recognized threats to the confidentiality, integrity, or availability of electronic protected health information; a sale, transfer, merger, or consolidation of all or part of the covered entity or business associate with another person; a security incident that affects the confidentiality, integrity, and availability of electronic protected health information; and relevant changes in Federal, State, Tribal, or territorial law.

(2) *Standard: Risk analysis*—(i) *General.* Conduct an accurate and comprehensive written assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all electronic protected health information created, received, maintained, or transmitted by the covered entity or business associate.

(ii) *Implementation specifications*—(A) *Assessment.* The written assessment must include, at a minimum, all of the following:

(*1*) A review of the technology asset inventory required by paragraph (a)(1)(ii)(A) of this section and the network map required by paragraph (a)(1)(ii)(B) of this section to identify where electronic protected health information may be created, received, maintained, or transmitted within the covered entity's or business associate's electronic information systems.

(*2*) Identification of all reasonably anticipated threats to the confidentiality, integrity, and availability of electronic protected health information that the covered entity or business associate creates, receives, maintains, or transmits.

(*3*) Identification of potential vulnerabilities and predisposing conditions to the covered entity's or business associate's relevant electronic information systems.

(*4*) An assessment and documentation of the security measures the covered entity or business associate uses to ensure the confidentiality, integrity, and availability of the electronic protected health information created, received, maintained, or transmitted by the covered entity or business associate.

(*5*) A reasonable determination of the likelihood that each threat identified in accordance with paragraph (a)(2)(ii)(A)(*2*) of this section will exploit the vulnerabilities identified in accordance with paragraph (a)(2)(ii)(A)(*3*) of this section.

(*6*) A reasonable determination of the potential impact of each threat identified in accordance with paragraph (a)(2)(ii)(A)(*2*) of this section successfully exploiting the vulnerabilities identified in accordance with paragraph (a)(2)(ii)(A)(*3*) of this section.

(*7*) An assessment of risk level for each threat identified in accordance with paragraph (a)(2)(ii)(A)(*2*) of this section and vulnerability identified in accordance with paragraph (a)(2)(ii)(A)(*3*) of this section, based on the determinations made in accordance with paragraphs (a)(2)(ii)(A)(*5*) and (*6*) of this section.

(*8*) An assessment of the risks to electronic protected health information posed by entering into or continuing a business associate contract or other written arrangement with any prospective or current business associate, respectively, based on the written verification obtained from the prospective or current business associate in accordance with paragraph (b)(1) of this section.

(B) *Maintenance.* Review, verify, and update the written assessment on an ongoing basis, but at least once every 12 months and, in accordance with paragraph (a)(1)(ii)(C)(*2*) of this section, in response to a change in the covered entity's or business associate's environment or operations that may affect electronic protected health information.

(3) *Standard: Evaluation*—(i) *General.* Perform a written technical and nontechnical evaluation to determine whether a change in the covered entity's or business associate's environment or operations may affect the confidentiality, integrity, or availability of electronic protected health information.

(ii) *Implementation specifications*—(A) *Performance.* Perform a written technical and nontechnical evaluation within a reasonable period of time before making a change in the covered entity's or business associate's environment or operations as described in paragraph (a)(1)(ii)(C)(*2*) of this section.

(B) *Response.* Respond to the written technical and nontechnical evaluation in accordance with the covered entity's or business associate's risk management plan required by paragraph (a)(5)(ii)(A) of this section.

(4) *Standard: Patch management*—(i) *General.* Implement written policies and procedures for applying patches and updating the configuration(s) of the covered entity's or business associate's relevant electronic information systems.

(ii) *Implementation specifications*—(A) *Policies and procedures.* Establish written policies and procedures for identifying, prioritizing, acquiring, installing, evaluating, and verifying the timely installation of patches, updates, and upgrades throughout the covered entity's or business associate's relevant electronic information systems.

(B) *Maintenance.* Review and test written policies and procedures required by paragraph (a)(4)(ii)(A) of this section at least once every 12 months, and modify such policies and procedures as reasonable and appropriate.

(C) *Application.* Patch, update, and upgrade the configurations of relevant electronic information systems in accordance with the written policies and procedures required by paragraph (a)(4)(ii)(A) of this section and based on the results of the covered entity's or business associate's risk analysis required by paragraph (a)(2) of this section, the vulnerability scans required by § 164.312(h)(2)(i), the monitoring of authoritative sources required by § 164.312(h)(2)(ii), and penetration tests required by § 164.312(h)(2)(iii), within a reasonable and appropriate period of time, as follows, except to the extent that an exception at paragraph (a)(4)(ii)(D) of this section applies:

(*1*) Within 15 calendar days of identifying the need to patch, update, or upgrade the configuration of a relevant electronic information system to address a critical risk in accordance with this paragraph (a)(4)(ii)(C), where a patch, update, or upgrade is available; or, where a patch, update, or upgrade is not available, within 15 calendar days of a patch, update, or upgrade becoming available.

(*2*) Within 30 calendar days of identifying the need to patch, update, or upgrade the configuration of a relevant electronic information system to address a high risk in accordance with this paragraph (a)(4)(ii)(C), where a patch, update, or upgrade is available; or, where a patch, update, or upgrade is not available, within 30 calendar days of a patch, update, or upgrade becoming available.

(*3*) As determined by and documented in the covered entity's or business associate's policies and procedures under paragraph (a)(4)(ii)(A) of this section for all other patches, updates, and upgrades to the configuration of a relevant electronic information system.

(D) *Exceptions.* This paragraph (a)(4)(ii)(D) applies only to the extent that a covered entity or business associate documents that an exception in this paragraph (a)(4)(ii)(D) applies and that all other applicable conditions are met.

(*1*) A patch, update, or upgrade to the configuration of a relevant electronic information system is not available to address a risk identified in the risk analysis under paragraph (a)(2) of this section.

(*2*) The only available patch, update, or upgrade would adversely affect the confidentiality, integrity, or availability of electronic protected health information.

(E) *Alternative measures.* Where an exception at paragraph (a)(4)(ii)(D) of this section applies, a covered entity or business associate must document in real-time the existence of an applicable exception and implement reasonable and appropriate compensating controls in accordance with paragraph (a)(4)(ii)(F) of this section.

(F) *Compensating controls.* To the extent that a covered entity or business associate determines that an exception at paragraph (a)(4)(ii)(D) of this section applies, a covered entity or business associate must implement reasonable and appropriate security measures to address the identified risk in a timely manner as required by paragraph (a)(5)(ii)(D) of this section until a patch, update, or upgrade that does not adversely affect the confidentiality, integrity, or availability of electronic protected health information becomes available.

(5) *Standard: Risk management*—(i) *General.* Implement security measures sufficient to reduce risks and vulnerabilities to all electronic protected health information to a reasonable and appropriate level.

(ii) *Implementation specifications*—(A) *Planning.* Establish and implement a written risk management plan for reducing risks to all electronic protected health information, including but not limited to those risks identified by the risk analysis under paragraph (a)(2)(ii)(A) of this section, to a reasonable and appropriate level.

(B) *Maintenance.* Review the written risk management plan required by paragraph (a)(5)(ii)(A) of this section at least once every 12 months and as reasonable and appropriate in response to changes in the risk analysis made in accordance with paragraph (a)(2)(ii)(B) of this section, and modify as reasonable and appropriate.

(C) *Priorities.* The written risk management plan must prioritize the risks identified in the risk analysis required by paragraph (a)(2)(ii)(A) of this section, based on the risk levels determined by such risk analysis.

(D) *Implementation.* Implement security measures in a timely manner to address the risks identified in the covered entity's or business associate's risk analysis in accordance with the priorities established under paragraph (a)(5)(ii)(C) of this section.

(6) *Standard: Sanction policy*—(i) *General.* Apply appropriate sanctions against workforce members who fail to comply with the security policies and

procedures of the covered entity or business associate.

(ii) *Implementation specifications*—(A) *Policies and procedures.* Establish written policies and procedures for sanctioning workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

(B) *Modifications.* Review written sanctions policies and procedures at least once every 12 months, and modify as reasonable and appropriate.

(C) *Application.* Apply and document appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate in accordance with the written policies and procedures for sanctioning workforce members required by paragraph (a)(6)(ii)(A) of this section.

(7) *Standard: Information system activity review*—(i) *General.* Implement written policies and procedures for regularly reviewing records of activity in the covered entity's or business associate's relevant electronic information systems.

(ii) *Implementation specifications*—(A) *Policies and procedures.* Establish written policies and procedures for retaining and reviewing records of activity in the covered entity's or business associate's relevant electronic information systems by persons and technology assets, including the frequency for reviewing such records.

(B) *Scope.* Records of activity in the covered entity's or business associate's relevant electronic information systems by persons and/or technology assets include but are not limited to audit trails, event logs, firewall logs, system logs, data backup logs, access reports, anti-malware logs, and security incident tracking reports.

(C) *Record review.* Review records of activity in a covered entity's or business associate's relevant electronic information systems by persons and technology assets as often as reasonable and appropriate for the type of report or log and document such review.

(D) *Record retention.* Retain records of activity in the covered entity's or business associate's relevant electronic information systems by persons and technology assets for a period of time that is reasonable and appropriate for the type of report or log.

(E) *Response.* Where a suspected or known security incident is identified during the review required by paragraph (a)(7)(ii)(C) of this section, respond in accordance with the covered entity's or business associate's security incident response plan required by paragraph (a)(12)(ii)(A)(*1*) of this section.

(F) *Maintenance.* Review and test the written policies and procedures required by paragraph (a)(7)(ii)(A) of this section at least once every 12 months and modify as reasonable and appropriate.

(8) *Standard: Assigned security responsibility.* In writing, identify the security official who is responsible for the development and implementation of the policies and procedures, written or otherwise, and deployment of technical controls required by this subpart for the covered entity or business associate.

(9) *Standard: Workforce security*—(i) *General.* Implement written policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information and relevant electronic information systems, and to prevent those workforce members who are not authorized to have access from obtaining access to electronic protected health information and relevant electronic information systems.

(ii) *Implementation specifications*—(A) *Authorization and/or supervision.* Establish and implement written procedures for the authorization and/or supervision of workforce members who access electronic protected health information or relevant electronic information systems, or who work in facilities where electronic protected health information or relevant electronic information systems might be accessed.

(B) *Workforce clearance procedure.* Establish and implement written procedures to determine that the access of a workforce member to electronic protected health information or relevant electronic information systems is appropriate in accordance with paragraph (a)(10)(ii)(B) of this section.

(C) *Modification and termination procedures.* (*1*) Establish and implement written procedures, in accordance with paragraph (a)(9)(ii)(C)(*2*) of this section, to terminate a workforce member's access to electronic protected health information and relevant electronic information systems, and to facilities where electronic protected health information or relevant electronic information systems might be accessed.

(*2*) A workforce member's access must be terminated as soon as possible but no later than one hour after the employment of, or other arrangement with, a workforce member ends.

(D) *Notification.* (*1*) Establish and implement written procedures, in accordance with paragraph (a)(9)(ii)(D)(*2*) of this section, to notify another covered entity or business associate of a change in or termination of access where the workforce member is or was authorized to access such electronic protected health information or relevant electronic information systems by the covered entity or business associate making the notification.

(*2*) Notification must occur as soon as possible but no later than 24 hours after a change in or termination of a workforce member's authorization to access electronic protected health information or relevant electronic information systems maintained by such other covered entity or business associate.

(E) *Maintenance.* Review and test written policies and procedures required under paragraph (a)(9)(ii)(A) through (D) of this section at least once every 12 months, and modify as reasonable and appropriate.

(10) *Standard: Information access management*—(i) *General.* Establish and implement written policies and procedures for authorizing access to electronic protected health information and relevant electronic information systems that are consistent with the applicable requirements of subpart E of this part.

(ii) *Implementation specifications*—(A) *Isolating health care clearinghouse functions.* If a health care clearinghouse is part of a larger organization, the clearinghouse must establish and implement written policies and procedures that protect the electronic protected health information and relevant electronic information systems of the clearinghouse from unauthorized access by the larger organization.

(B) *Access authorization.* Establish and implement written policies and procedures for granting and revising access to electronic protected health information and relevant electronic information systems as necessary and appropriate for each prospective user and technology asset to carry out their assigned function(s).

(C) *Authentication management.* Establish and implement written policies and procedures for verifying the identities of users and technology assets prior to accessing the covered entity's or business associate's relevant electronic information systems, including written policies and procedures for implementing multi-factor authentication technical controls required by § 164.312(f)(2)(ii) through (v).

(D) *Access determination and modification.* Establish and implement written policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, determine, document, review, and modify the access of each user and technology asset to specific components

of the covered entity's or business associate's relevant electronic information systems.

(E) *Network segmentation.* Establish and implement written policies and procedures that ensure that a covered entity's or business associate's relevant electronic information systems are segmented to limit access to electronic protected health information to authorized workstations.

(F) *Maintenance.* Review and test the written policies and procedures required by this paragraph (a)(10)(ii) at least once every 12 months, and modify as reasonable and appropriate.

(11) *Standard: Security awareness training*—(i) *General.* Implement security awareness training for all workforce members on protection of electronic protected health information and information systems as necessary and appropriate for the members of the workforce to carry out their assigned function(s).

(ii) *Implementation specifications*—(A) *Training.* A covered entity or business associate must develop and implement security awareness training for all workforce members that addresses all of the following:

(*1*) The written policies and procedures with respect to electronic protected health information required by this subpart as necessary and appropriate for the workforce members to carry out their assigned functions.

(*2*) Guarding against, detecting, and reporting suspected or known security incidents, including but not limited to, malicious software and social engineering.

(*3*) The written policies and procedures for accessing the covered entity's or business associate's relevant electronic information systems, including but not limited to: safeguarding passwords; setting unique passwords of sufficient strength to ensure the confidentiality, integrity, and availability of electronic protected health information; and limitations on sharing passwords.

(B) *Timing.* A covered entity or business associate must provide security awareness training as follows:

(*1*) As required by paragraph (a)(11)(ii)(A) of this section, to each member of its workforce by no later than the compliance date, and at least once every 12 months thereafter.

(*2*) As required by paragraph (a)(11)(ii)(A) of this section, to each new member of its workforce within a reasonable period of time but no later than 30 days after the person first has access to the covered entity's or business associate's relevant electronic information systems.

(*3*) On a material change to the policies or procedures required by this subpart, to each member of its workforce whose functions are affected by such change, within a reasonable period of time but no later than 30 days after the material change occurs.

(C) *Ongoing education.* A covered entity or business associate must provide its workforce members ongoing reminders of their security responsibilities and notifications of relevant threats, including but not limited to new and emerging malicious software and social engineering.

(D) *Documentation.* A covered entity or business associate must document that the training required by paragraph (a)(11)(ii)(A) of this section and ongoing reminders required by paragraph (a)(11)(ii)(C) of this section have been provided.

(12) *Standard: Security incident procedures*—(i) *General.* Implement written policies and procedures to respond to security incidents.

(ii) *Implementation specifications*—(A) *Planning and testing.* (*1*) Establish written security incident response plan(s) and procedures documenting how workforce members are to report suspected or known security incidents and how the covered entity or business associate will respond to suspected or known security incidents in accordance with paragraph (a)(12)(ii)(B) of this section.

(*2*) Implement written procedures for testing and revising security incident response plan(s) required by paragraph (a)(12)(ii)(A)(*1*) of this section.

(*3*) Review and test security incident response plan(s) and procedures required by paragraph (a)(12)(ii)(A)(*1*) of this section at least once every 12 months, document the results of such tests, and modify security incident response plan(s) and procedures as reasonable and appropriate.

(B) *Response.* (*1*) Identify and respond to suspected or known security incidents.

(*2*) Mitigate, to the extent practicable, harmful effects of security incidents that are suspected or known to the covered entity or business associate.

(*3*) Identify and remediate, to the extent practicable, the root cause(s) of security incidents that are suspected or known to the covered entity or business associate.

(*4*) Eradicate the security incidents that are suspected or known to the covered entity or business associate.

(*5*) For suspected and known security incidents, develop and maintain documentation of investigations, analyses, mitigation, and remediation.

(13) *Standard: Contingency plan*—(i) *General.* Establish and implement as needed a written contingency plan, consisting of written policies and procedures for responding to an emergency or other occurrence—including but not limited to fire, vandalism, system failure, natural disaster, or security incident—that adversely affects relevant electronic information systems.

(ii) *Implementation specifications*—(A) *Criticality analysis.* Perform and document an assessment of the relative criticality of the covered entity's or business associate's relevant electronic information systems and technology assets in its relevant electronic information systems.

(B) *Data backups.* Establish and implement written procedures to create and maintain exact retrievable copies of electronic protected health information, including verification that the electronic protected health information has been copied accurately.

(C) *Information systems backups.* Establish and implement written procedures to create and maintain backups of the covered entity's or business associate's relevant electronic information systems, including verification of success of backups.

(D) *Disaster recovery plan.* (*1*) Establish (and implement as needed) written procedures to restore loss of the covered entity's or business associate's critical relevant electronic information systems and data within 72 hours of the loss.

(*2*) Establish (and implement as needed) written procedures to restore loss of the covered entity's or business associate's other relevant electronic information systems and data in accordance with the criticality analysis required by paragraph (a)(13)(ii)(A) of this section.

(E) *Emergency mode operation plan.* Establish (and implement as needed) written procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(F) *Testing and revision procedures.* (*1*) Establish written procedures for testing and revising contingency plans as required by this paragraph (a)(13) in accordance with paragraph (a)(13)(ii)(F)(*2*) of this section.

(*2*) Review and test contingency plans required by this paragraph (a)(13) at least once every 12 months, document the results of such tests, and modify such contingency plans as reasonable and appropriate in accordance with the results of those tests.

(14) *Standard: Compliance audit.* Perform and document an audit at least once every 12 months of the covered entity's or business associate's compliance with each standard and implementation specification in this subpart.

(b)(1) *Standard: Business associate contracts and other arrangements.* (i)(A) 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 comply with this subpart and verifies that the business associate has deployed technical safeguards in accordance with the requirements of § 164.312.

(B) A covered entity is not required to obtain such satisfactory assurances or verification from a business associate that is a subcontractor.

(ii) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will comply with the requirements of this subpart and verifies that the business associate that is a subcontractor has deployed technical safeguards in accordance with the requirements of § 164.312.

(2) *Implementation specifications*—(i) *Written contract or other arrangement.* Document the satisfactory assurances required by paragraph (b)(1)(i) or (ii) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

(ii) *Written verification.* Obtain written verification from the business associate at least once every 12 months that the business associate has deployed the technical safeguards as required by § 164.312 through both of the following:

(A) A written analysis of the business associate's relevant electronic information systems by a person with appropriate knowledge of and experience with generally accepted cybersecurity principles and methods for ensuring the confidentiality, integrity, and availability of electronic protected health information to verify compliance with each standard and implementation specification in § 164.312.

(B) A written certification that the analysis has been performed and is accurate by a person who has the authority to act on behalf of the business associate.

(3) *Standard: Delegation to business associate.* (i) A covered entity or business associate may permit a business associate to serve as their designated security official.

(ii) A covered entity or business associate that delegates actions, activities, or assessments required by this subpart to a business associate remains liable for compliance with all applicable provisions of this subpart.

§ 164.310 Physical safeguards.

Each covered entity and business associate must, in accordance with §§ 164.306 and 164.316, implement all of the following physical safeguards to protect the confidentiality, integrity, and availability of all electronic protected health information that it creates, receives, maintains, or transmits:

(a) *Standard: Facility access controls*—(1) *General.* Establish and implement written policies and procedures to limit physical access to all of its relevant electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(2) *Implementation specifications*—(i) *Contingency operations.* Establish (and implement as needed) written procedures that allow facility access in support of the covered entity's or business associate's contingency plan required by § 164.308(a)(13).

(ii) *Facility security plan.* Establish and implement written policies and procedures to safeguard all facilities and the equipment therein from unauthorized physical access, tampering, and theft.

(iii) *Access management and validation procedures.* Establish and implement written procedures to authorize and manage a person's access to facilities based on their role or function, including visitor management.

(iv) *Physical maintenance records.* Establish and implement written policies and procedures to document repairs and modifications to the physical components of a facility that are related to security, including but not limited to hardware, walls, doors, locks, and security cameras.

(v) *Maintenance.* For each facility, review and test the written policies and procedures required by this paragraph (a)(2) at least once every 12 months, and modify such policies and procedures as reasonable and appropriate.

(b) *Standard: Workstation use*—(1) *General.* Establish and implement written policies and procedures that govern the use of workstations that access electronic protected health information or the covered entity's or business associate's relevant electronic information systems.

(2) *Implementation specifications*—(i) *Policies and procedures.* The written policies and procedures must specify all of the following with respect to a workstation that accesses electronic protected health information or the covered entity's or business associate's relevant electronic information systems:

(A) The functions for which a workstation may be used.

(B) The manner in which a workstation may be used to perform those functions.

(C) The physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information, including the removal of such workstations from a facility and the movement of such workstations within and outside of a facility.

(ii) *Maintenance.* Review and test written policies and procedures at least once every 12 months, and modify as reasonable and appropriate.

(c) *Standard: Workstation security.* Implement and modify physical safeguards for all workstations that access electronic protected health information or relevant electronic information systems, to address the written policies and procedures for workstation use required by paragraph (b) of this section and restrict access to authorized users.

(d) *Standard: Technology asset controls*—(1) *General.* Establish and implement written policies and procedures that govern the receipt and removal of technology assets that maintain electronic protected health information into and out of a facility, and the movement of these assets within the facility.

(2) *Implementation specifications*—(i) *Disposal.* Establish and implement written policies and procedures for disposal of electronic protected health information and the technology assets on which it is maintained based on current standards for disposing of such technology assets.

(ii) *Media sanitization.* Establish and implement written procedures for removal of electronic protected health information from electronic media such that the electronic protected health information cannot be recovered, based on current standards for sanitizing electronic media before the media are made available for re-use.

(iii) *Maintenance.* Review and test the written policies and procedures required by paragraphs (d)(2)(i) and (ii)

of this section at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

§ 164.312 Technical safeguards.

Each covered entity or business associate must, in accordance with §§ 164.306 and 164.316, implement all of the following technical safeguards, including technical controls, to protect the confidentiality, integrity, and availability of all electronic protected health information that it creates, receives, maintains, or transmits:

(a) *Standard: Access control*—(1) *General.* Deploy technical controls in relevant electronic information systems to allow access only to users and technology assets that have been granted access rights.

(2) *Implementation specifications*—(i) *Unique identification.* Assign a unique name, number, and/or other identifier for tracking each user and technology asset in the covered entity or business associate's relevant electronic information systems.

(ii) *Administrative and increased access privileges.* Separate user identities from identities used for administrative and other increased access privileges.

(iii) *Emergency access procedure.* Establish (and implement as needed) written and technical procedures for obtaining necessary electronic protected health information during an emergency.

(iv) *Automatic logoff.* Deploy technical controls that terminate an electronic session after a predetermined time of inactivity that is reasonable and appropriate.

(v) *Log-in attempts.* Deploy technical controls that disable or suspend the access of a user or technology asset to relevant electronic information systems after a reasonable and appropriate predetermined number of unsuccessful authentication attempts.

(vi) *Network segmentation.* Deploy technical controls to ensure that the covered entity's or business associate's relevant electronic information systems are segmented in a reasonable and appropriate manner.

(vii) *Data controls.* Deploy technical controls to allow access to electronic protected health information only to those users and technology assets that have been granted access rights to the covered entity's or business associate's relevant electronic information systems as specified in § 164.308(a)(10).

(viii) *Maintenance.* Review and test the effectiveness of the procedures and technical controls required by this paragraph (a)(2) at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

(b) *Standard: Encryption and decryption*—(1) *General.* Deploy technical controls to encrypt and decrypt electronic protected health information using encryption that meets prevailing cryptographic standards.

(2) *Implementation specification.* Encrypt all electronic protected health information at rest and in transit, except to the extent that an exception at paragraph (b)(3) of this section applies.

(3) *Exceptions.* This paragraph (b)(3) applies only to the electronic protected health information directly affected by one or more of the following exceptions and only to the extent that the covered entity or business associate documents that an exception applies and that all other applicable conditions are met.

(i) The technology asset in use does not support encryption of the electronic protected health information consistent with prevailing cryptographic standards, and the covered entity or business associate establishes and implements a written plan to migrate electronic protected health information to a technology asset that supports encryption consistent with prevailing cryptographic standards within a reasonable and appropriate period of time.

(ii) An individual requests pursuant to § 164.524 to receive their electronic protected health information in an unencrypted manner and has been informed of the risks associated with the transmission, receipt, and storage of unencrypted electronic protected health information. This exception does not apply where such individual will receive their electronic protected health information pursuant to § 164.524 and the technology used by the individual to receive the electronic protected health information is controlled by the covered entity or its business associate.

(iii) During an emergency or other occurrence that adversely affects the covered entity's or business associate's relevant electronic information systems in which encryption is infeasible, and the covered entity or business associate implements reasonable and appropriate compensating controls in accordance with and determined by the covered entity's or business associate's contingency plan under § 164.308(a)(13).

(iv) The technology asset in use is a device under section 201(h) of the Food, Drug, and Cosmetic Act, 21 U.S.C. 321(h) that has been authorized for marketing by the Food and Drug Administration, as follows:

(A) Pursuant to a submission received before March 29, 2023, provided that the covered entity or business associate deploys in a timely manner any updates or patches required or recommended by the manufacturer of the device.

(B) Pursuant to a submission received on or after March 29, 2023, where the device is no longer supported by its manufacturer, provided that the covered entity or business associate has deployed any updates or patches required or recommended by the manufacturer of the device.

(C) Pursuant to a submission received on or after March 29, 2023, where the device is supported by its manufacturer.

(4) *Alternative measures*—(i) *Alternative measures.* Where an exception at paragraph (b)(3) of this section applies, a covered entity or business associate must document in real-time the existence of an applicable exception and implement reasonable and appropriate compensating controls in accordance with paragraph (b)(4)(ii) of this section.

(ii) *Compensating controls.* (A) To the extent that a covered entity or business associate determines that an exception at paragraph (b)(3)(i), (ii), or (iii) or (b)(3)(iv)(A) or (B) of this section applies, the covered entity or business associate must secure such electronic protected health information by implementing reasonable and appropriate compensating controls reviewed and approved by the covered entity's or business associate's designated Security Official.

(B) To the extent that a covered entity or business associate determines that an exception at paragraph (b)(3)(iv)(C) of this section applies, the covered entity or business associate shall be presumed to have implemented reasonable and appropriate compensating controls where the covered entity or business associate has deployed the security measures prescribed and as instructed by the authorized label for the device, including any updates or patches recommended or required by the manufacturer of the device.

(C) To the extent that a covered entity or business associate is implementing compensating controls under this paragraph (b)(4)(ii), the implementation and effectiveness of compensating controls must be reviewed, documented, and signed by the designated Security Official at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, to continue securing electronic protected health information and relevant electronic information systems.

(5) *Maintenance.* Review and test the effectiveness of the technical controls required by this paragraph (b) at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

(c) *Standard: Configuration management*—(1) *General.* Establish and deploy technical controls for securing the covered entity's or business associate's relevant electronic information systems and technology assets in its relevant electronic information systems, including workstations, in a consistent manner, and maintain such electronic information systems and technology assets according to the covered entity's or business associate's established secure baselines.

(2) *Implementation specifications*—(i) *Anti-malware protection.* Deploy technology assets and/or technical controls that protect all of the covered entity's or business associate's technology assets in its relevant electronic information systems against malicious software, including but not limited to viruses and ransomware.

(ii) *Software removal.* Remove extraneous software from the covered entity's or business associate's relevant electronic information systems.

(iii) *Configuration.* Configure and secure operating system(s) and software consistent with the covered entity's or business associate's risk analysis under § 164.308(a)(2).

(iv) *Network ports.* Disable network ports in accordance with the covered entity's or business associate's risk analysis under § 164.308(a)(2).

(v) *Maintenance.* Review and test the effectiveness of the technical controls required by this paragraph (c) at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

(d) *Standard: Audit trail and system log controls*—(1) *General.* Deploy technology assets and/or technical controls that record and identify activity in the covered entity's or business associate's relevant electronic information systems.

(2) *Implementation specifications*—(i) *Monitor and identify.* The covered entity or business associate must deploy technology assets and/or technical controls that monitor in real-time all activity in its relevant electronic information systems, identify indications of unauthorized persons or unauthorized activity as determined by the covered entity's or business associate's risk analysis under § 164.308(a)(2), and alert workforce members of such indications in accordance with the policies and procedures required by § 164.308(a)(7).

(ii) *Record.* The covered entity or business associate must deploy technology assets and/or technical controls that record in real-time all activity in its relevant electronic information systems.

(iii) *Retain.* The covered entity or business associate must deploy technology assets and/or technical controls to retain records of all activity in its relevant electronic information systems as determined by the covered entity's or business associate's policies and procedures for information system activity review at § 164.308(a)(7)(ii)(A).

(iv) *Scope.* Activity includes creating, accessing, receiving, transmitting, modifying, copying, or deleting any of the following:

(A) Electronic protected health information.

(B) Relevant electronic information systems and the information therein.

(v) *Maintenance.* Review and test the effectiveness of the technology assets and/or technical controls required by this paragraph (d) at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

(e) *Standard: Integrity.* Deploy technical controls to protect electronic protected health information from improper alteration or destruction, both at rest and in transit; and review and test the effectiveness of such technical controls at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

(f) *Standard: Authentication*—(1) *General.* Deploy technical controls to verify that a person or technology asset seeking access to electronic protected health information and/or the covered entity's or business associate's relevant electronic information systems is the one claimed.

(2) *Implementation specifications*—(i) *Information access management policies.* Deploy technical controls in accordance with the covered entity's or business associate's information access management policies and procedures under § 164.308(a)(10), including technical controls that require users to adopt unique passwords that are consistent with the current recommendations of authoritative sources.

(ii) *Multi-factor authentication.* (A) Deploy multi-factor authentication to all technology assets in the covered entity's or business associate's relevant electronic information systems to verify that a person seeking access to the relevant electronic information system(s) is the user that the person claims to be.

(B) Deploy multi-factor authentication for any action that would change a user's privileges to the covered entity's or business associate's relevant electronic information systems in a manner that would alter the user's ability to affect the confidentiality, integrity, or availability of electronic protected health information.

(iii) *Exceptions.* Deployment of multi-factor authentication is not required in any of the following circumstances.

(A) The technology asset in use does not support multi-factor authentication, and the covered entity or business associate establishes and implements a written plan to migrate electronic protected health information to a technology asset that supports multi-factor authentication within a reasonable and appropriate period of time.

(B) During an emergency or other occurrence that adversely affects the covered entity's or business associate's relevant electronic information systems or the confidentiality, integrity, or availability of electronic protected health information in which multi-factor authentication is infeasible and the covered entity or business associate implements reasonable and appropriate compensating controls in accordance with its emergency access procedures under paragraph (a)(2)(iii) of this section and the covered entity's or business associate's contingency plan under § 164.308(a)(13).

(C) The technology asset in use is a device under section 201(h) of the Food, Drug, and Cosmetic Act, 21 U.S.C. 321(h) that has been authorized for marketing by the Food and Drug Administration, as follows:

(*1*) Pursuant to a submission received before March 29, 2023, provided that the covered entity or business associate has deployed any updates or patches required or recommended by the manufacturer of the device.

(*2*) Pursuant to a submission received on or after March 29, 2023, where the device is no longer supported by its manufacturer, provided that the covered entity or business associate has deployed any updates or patches required or recommended by the manufacturer of the device.

(*3*) Pursuant to a submission received on or after March 29, 2023, where the device is supported by its manufacturer.

(iv) *Alternative measures*—(A) *Alternative measures.* Where an exception at paragraph (f)(2)(iii) of this

section applies, a covered entity or business associate must document in real-time the existence of an applicable exception and implement reasonable and appropriate compensating controls as required by paragraph (f)(2)(iv)(B) of this section.

(B) *Compensating controls.* (*1*) To the extent that a covered entity or business associate determines that an exception at paragraph (f)(2)(iii)(A) or (B) or (f)(2)(iii)(C)(*1*) or (*2*) of this section applies, the covered entity or business associate must secure its relevant electronic information systems by implementing reasonable and appropriate compensating controls reviewed, approved, and signed by the covered entity's or business associate's designated Security Official.

(*2*) To the extent that a covered entity or business associate determines that an exception at paragraph (f)(2)(iii)(C)(*3*) of this section applies, the covered entity or business associate shall be presumed to have implemented reasonable and appropriate compensating controls where the covered entity or business associate has deployed the security measures prescribed and as instructed by the authorized label for the device, including any updates or patches recommended or required by the manufacturer of the device.

(*3*) To the extent that a covered entity or business associate is implementing compensating controls under this paragraph (f)(2)(iv)(B), the effectiveness of compensating controls must be reviewed and documented by the designated Security Official at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, to continue securing electronic protected health information and its relevant electronic information systems.

(v) *Maintenance.* Review and test the effectiveness of the technical controls required by this paragraph (f) at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

(g) *Standard: Transmission security.* Deploy technical controls to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network; and review and test the effectiveness of such technical controls at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

(h) *Standard: Vulnerability management*—(1) *General.* Deploy technical controls in accordance with the covered entity's or business associate's patch management policies and procedures required by § 164.308(a)(4)(ii)(A) to identify and address technical vulnerabilities in the covered entity's or business associate's relevant electronic information systems.

(2) *Implementation specifications*—(i) *Vulnerability scanning.* (A) Conduct automated vulnerability scans to identify technical vulnerabilities in the covered entity's or business associate's relevant electronic information systems in accordance with the covered entity's or business associate's risk analysis required by § 164.308(a)(2) or at least once every six months, whichever is more frequent.

(B) Review and test the effectiveness of the technology asset(s) that conducts the automated vulnerability scans required by paragraph (h)(2)(i)(A) of this section at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

(ii) *Monitoring.* Monitor authoritative sources for known vulnerabilities on an ongoing basis and remediate such vulnerabilities in accordance with the covered entity's or business associate's patch management program under § 164.308(a)(4).

(iii) *Penetration testing.* Perform penetration testing of the covered entity's or business associate's relevant electronic information systems by a qualified person.

(A) A qualified person is a person with appropriate knowledge of and experience with generally accepted cybersecurity principles and methods for ensuring the confidentiality, integrity, and availability of electronic protected health information.

(B) Penetration testing must be performed at least once every 12 months or in accordance with the covered entity's or business associate's risk analysis required by § 164.308(a)(2), whichever is more frequent.

(iv) *Patch and update installation.* Deploy technical controls in accordance with the covered entity's or business associate's patch management program under § 164.308(a)(4) to ensure timely installation of software patches and critical updates as reasonable and appropriate.

(i) *Standard: Data backup and recovery*—(1) *General.* Deploy technical controls to create and maintain exact retrievable copies of electronic protected health information.

(2) *Implementation specifications*—(i) *Data backup.* Create backups of electronic protected health information in accordance with the policies and procedures required by § 164.308(a)(13)(ii)(B) and with such frequency to ensure retrievable copies of electronic protected health information are no more than 48 hours older than the electronic protected health information maintained in the covered entity or business associate's relevant electronic information systems.

(ii) *Monitor and identify.* Deploy technical controls that, in real-time, monitor, and alert workforce members about, any failures and error conditions of the backups required by paragraph (i)(2)(i) of this section.

(iii) *Record.* Deploy technical controls that record the success, failure, and any error conditions of backups required by paragraph (i)(2)(i) of this section.

(iv) *Testing.* Restore a representative sample of electronic protected health information backed up as required by paragraph (i)(2)(i) of this section, and document the results of such test restorations at least monthly.

(j) *Standard: Information systems backup and recovery.* Deploy technical controls to create and maintain backups of relevant electronic information systems; and review and test the effectiveness of such technical controls at least once every six months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

§ 164.314 Organizational requirements.

(a)(1) *Standard: Business associate contracts or other arrangements.* The contract or other arrangement required by § 164.308(b)(2) must meet the requirements of paragraph (a)(2)(i), (ii), or (iii) of this section, as applicable.

(2) *Implementation specifications*—(i) *Business associate contracts.* The contract must provide that the business associate will do all of the following:

(A) Comply with the applicable requirements of this subpart.

(B) In accordance with § 164.308(b)(1)(ii), 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.

(C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured electronic protected health information as required by § 164.410.

(D) Report to the covered entity activation of its contingency plan under § 164.308(a)(13) without unreasonable

delay, and in no case later than 24 hours after activation of the contingency plan.

(ii) *Other arrangements.* 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).

(iii) *Business associate contracts with subcontractors.* The requirements of paragraphs (a)(2)(i) and (ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(1)(ii) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

(b)(1) *Standard: 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.

(2) *Implementation specifications.* The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to do all of the following:

(i) *Safeguard implementation.* Implement the administrative, physical, and technical safeguards that covered entities and business associates are required to implement under §§ 164.308(a), 164.310, and 164.312.

(ii) *Separation.* Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by the administrative, physical, and technical safeguards implemented in accordance with paragraph (b)(2)(i) of this section.

(iii) *Agents.* Ensure that any agent to whom it provides this information agrees to implement the administrative, physical, and technical safeguards in accordance with paragraph (b)(2)(i) of this section.

(iv) *Security incident awareness.* Report to the group health plan any security incident of which it becomes aware.

(v) *Contingency plan activation.* Report to the group health plan activation of its contingency plan, adopted in accordance with § 164.308(a)(13) as required by paragraph (b)(2)(i) of this section, without unreasonable delay and in no case later than 24 hours after activation of the contingency plan.

§ 164.316 Documentation requirements.

(a) *Standard: Documentation.* A covered entity or business associate must do all of the following in written form, which may be electronic, taking into consideration the factors in § 164.306(b):

(1) Document the policies and procedures required to comply with this subpart and how the covered entity or business associate considered the factors at § 164.306(b) in the development of such policies and procedures.

(2) Document each action, activity, or assessment required by this subpart.

(b) *Implementation specifications*—(1) *Time limit.* Retain the documentation required by paragraph (a) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

(2) *Availability.* Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

(3) *Updates.* Review and update documentation at least once every 12 months and within a reasonable and appropriate period of time after a security measure is modified.

§ 164.318 Transition provisions.

(a) *Standard: Effect of prior contracts or other arrangements with business associates.* Notwithstanding any other provisions of this subpart, a covered entity, or business associate with respect to a subcontractor, may allow a business associate to create, receive, maintain, or transmit electronic protected health information pursuant to a written contract or other arrangement with such business associate that does not comply with §§ 164.308(b) and 164.314(a), only in accordance with paragraph (b) of this section.

(b) *Implementation specification: Deemed compliance*—(1) *Qualification.* Notwithstanding other sections of this subpart, a covered entity, or business associate with respect to a subcontractor, is deemed to be in compliance with the documentation and contract requirements of §§ 164.308(b) and 164.314(a), with respect to a particular business associate relationship for the time period set forth in paragraph (b)(2) of this section, if both of the following apply:

(i) Prior to [DATE OF PUBLICATION OF THE FINAL RULE IN THE **Federal Register**], such covered entity, or business associate with respect to a subcontractor, has entered into and is operating pursuant to a written contract or other written arrangement with the business associate that complies with the applicable provisions of §§ 164.308(b) and 164.314(a) that were in effect on such date.

(ii) The contract or other arrangement is not renewed or modified from [DATE 60 DAYS AFTER DATE OF PUBLICATION OF THE FINAL RULE IN THE **Federal Register**], until [DATE 240 DAYS AFTER DATE OF PUBLICATION OF THE FINAL RULE IN THE **Federal Register**].

(2) *Limited deemed compliance period.* A prior contract or other arrangement that meets the qualification requirements at paragraph (b)(1) of this section shall be deemed compliant until the earlier of the following dates:

(i) The date such contract or other arrangement is renewed on or after [DATE 240 DAYS AFTER DATE OF PUBLICATION OF THE FINAL RULE IN THE **Federal Register**].

(ii) [DATE 1 YEAR AND 60 DAYS AFTER DATE OF PUBLICATION OF THE FINAL RULE IN THE **Federal Register**].

(c) *Covered entity and business associate responsibilities.* Nothing in this section shall alter the requirements of a covered entity or business associate to comply with applicable provisions of this part other than §§ 164.308(b) and 164.314(a).

§ 164.320 Severability.

If any provision of this subpart is held to be invalid or unenforceable by its terms, or as applied to any person or circumstance, or stayed pending further agency action, it shall be construed so as to give it maximum effect permitted by law, unless such holding shall be one of utter invalidity or unenforceability, in which event such provision shall be severable from this subpart and shall not affect the remainder thereof or the application of such provision to other persons not similarly situated or to other dissimilar circumstances.

Appendix A to Subpart C of Part 164—
Security Standards: Matrix

Standards	Sections	Implementation specifications
Administrative Safeguards		
Technology asset inventory	164.308(a)(1)	Inventory. Network map. Maintenance.
Risk analysis	164.308(a)(2)	Assessment Maintenance.
Evaluation	164.308(a)(3)	Performance Response.
Patch Management	164.308(a)(4)	Policies and procedures. Maintenance. Application. Exceptions. Alternative measures. Compensating controls.
Risk management	164.308(a)(5)	Planning. Maintenance. Priorities. Implementation.
Sanction policy	164.308(a)(6)	Policies and procedures. Modifications. Application.
Information system activity review	164.308(a)(7)	Policies and procedures. Scope. Record review. Record retention. Response. Maintenance.
Assigned security responsibility	164.308(a)(8)	
Workforce security	164.308(a)(9)	Authorization and/or supervision. Workforce clearance procedure. Modification and termination procedures. Notification. Maintenance.
Information access management	164.308(a)(10)	Isolating health care clearinghouse functions. Access authorization. Authentication management. Access determination and modification. Network segmentation. Maintenance.
Security awareness training	164.308(a)(11)	Training. Timing. Ongoing education. Documentation.
Security incident procedures	163.308(a)(12)	Planning and testing. Response.
Contingency plan	163.308(a)(13)	Criticality analysis. Data backups. Information systems backups. Disaster recovery plan. Emergency mode operation plan. Testing and revision procedures.
Compliance audit	164.308(a)(14)	
Business associate contracts and other arrangements	164.308(b)(1)	Written contract or other arrangement. Written verification.
Delegation to business associate	164.308(b)(3)	
Physical Safeguards		
Facility access controls	164.310(a)	Contingency operations. Facility security plan. Access management and validation procedures. Physical maintenance records. Maintenance.
Workstation use	164.310(b)	Policies and procedures. Maintenance.
Workstation security	164.310(c)	
Technology asset controls	164.310(d)	Disposal. Media sanitization. Maintenance.

Standards	Sections	Implementation specifications
Technical Safeguards		
Access control	164.312(a)	Unique identification. Administrative and increased access privileges. Emergency access procedure. Automatic logoff. Log-in attempts. Network segmentation. Data controls. Maintenance.
Encryption and decryption	164.312(b)	Implementation specification. Exceptions. Alternative measures. Compensating controls. Maintenance.
Configuration management	164.312(c)	Anti-malware protection. Software removal. Configuration. Network ports. Maintenance.
Audit trail and system log controls	164.312(d)	Monitor and identify. Record. Retain. Scope. Maintenance.
Integrity	164.312(e)	
Authentication	164.312(f)	Information access management policies. Multi-factor authentication. Exceptions. Alternative measures. Compensating controls. Maintenance.
Transmission security	164.312(g)	
Vulnerability management	164.312(h)	Vulnerability scanning. Monitoring. Penetration testing. Patch and update installation.
Data backup and recovery	164.312(i)	Data backup Monitor and identify. Record. Testing.
Information systems backup and recovery	164.312(j)	

Dated: December 20, 2024.

Xavier Becerra,

Secretary, Department of Health and Human Services.

[FR Doc. 2024–30983 Filed 12–27–24; 4:15 pm]

BILLING CODE 4153–01–P