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 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.[1] 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.[2]
- Procedures for guarding against, detecting, and reporting malicious software.[436]
- Procedures for monitoring log-in attempts and reporting discrepancies.[3]
- Procedures for creating, changing, and safeguarding passwords.[4]

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

[1] *See* 45 CFR 164.502(b) and 164.514(d).
[2] 45 CFR 164.308(a)(5)(ii)(A). [436]
45 CFR 164.308(a)(5)(ii)(B).
[3] 45 CFR 164.308(a)(5)(ii)(C).
[4] 45 CFR 164.308(a)(5)(ii)(D).

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.[5] 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

[5] 45 CFR 164.308(a)(7)(ii)(A). [440] 45 CFR 164.308(a)(7)(ii)(B).

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.[6]

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 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.[7] 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

[6] 45 CFR 164.308(b)(3).

[7] *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.

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.[8] 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.[9] 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.[10]

3. Proposals

---

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

[9] *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").

[10] *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,

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,

---

2024), https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incidentfrequently-asked-questions/index.html.

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 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.[11] 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

[11] *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/specialtopics/health-information-technology/cloud-computing/index.html.

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,[12] 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.[13]

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.[14] 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.[15]

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.[16] 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.[17]

---

[12] "Cybersecurity Performance Goals," *supra* note 18.
[13] *See* Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 5.
[14] *See* 68 FR 8333, 8352 (Feb. 20, 2003).
[15] *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/forprofessionals/security/guidance/cybersecurity-newsletter-summer-2020/index.html.
[16] *Id*.
[17] *See* "The NIST Cybersecurity Framework (CSF) 2.0," *supra* note 15, p. 3.

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.[18] It would also be required to include the identification, version, person accountable for, and location of each of the assets or information system components.[19]

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 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,

[18] Proposed 45 CFR 164.308(a)(1)(ii)(A).
[19] *Id.*

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.[20]

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.

[20] *See, e.g.*, "New York State Register," *supra* note 14.

- 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.[21]

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.[22] 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[23] (IoT)) and provides access to facilities for maintenance personnel to control and

---

[21] "Making a List and Checking it Twice: HIPAA and IT Asset Inventories," *supra* note 451.
[22] *Id.*
[23] 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.

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.[2425] Basic questions that a regulated entity would consider when conducting a risk analysis that is compliant with the Security Rule include:[26]

- 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?

[24] *See* "Guidance on Risk Analysis," Office for Civil Rights, U.S. Department of Health and Human Services (July [25] , 2019), https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-riskanalysis/index.html?language=es.

[26] *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 human, natural, and environmental threats to information systems that contain ePHI?
- 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.[27] The Department has issued multiple guidance documents and tools for regulated entities to help them implement risk analyses,[28] and several versions of its Security Risk Assessment Tool, a desktop application that walks users through the process of conducting a risk assessment.[29] NIST has published numerous guides for risk assessment over the past two decades,[30] 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,[31] and "how to" guides on risk analysis.[32] In February 2024, NIST released a new guide that provides resources for implementing a Security Rule risk analysis.[33] 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.[34] 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

---

[27] *See* "Guidance on Risk Analysis," *supra* note 460.
[28] *See id.*
[29] *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.
[30] *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-informationtechnology/hipaa-security-rule.
[31] *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/hhsguidance-documents//nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf.
[32] "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide," *supra* note 461.
[33] *See id*.
[34] 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.

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.[35] While a risk analysis is a comprehensive identification of risks and vulnerabilities to all ePHI, a gap

[35] "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/cybersecuritynewsletter-april-2018.pdf.

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.[36] 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.[37] 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

---

[36] Joint Task Force, "Guide for Conducting Risk Assessments," NIST Special Publication 800-30, Revision 1, National Institute of Standards and Technology, U.S. Department of Commerce (Sept. 2012), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[37] *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.

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.[38] 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.[39] 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.

[38] *See* "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide," *supra* note 461, p. 16-22.
[39] "2016-2017 HIPAA Audits Industry Report," *supra* note 121.

- 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.[40] 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.[41]

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

---

[40] *Id.*

[41] 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://prodwwwhhsgov.cloud.hhs.gov/about/news/2024/07/01/hhs-office-civil-rights-settles-hipaa-security-rule-failures950000.html.

ring.[42] 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.[43] The cyberattack affected the ePHI of over 200,000 individuals when the business

[42] *See* "Montefiore Medical Center," *supra* note 248.
[43] *See* "Doctors' Management Services, Inc.," *supra* note 246.

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,[44] 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:[4546]

- 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.[47]

---

[44] *See* Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 4-6.
[45] Proposed 45 CFR 164.308(a)(2)(ii)(A).
[46]).
[47] Proposed 45 CFR 164.308(a)(2)(ii)(A)(*2*).
Proposed 45 CFR 164.308(a)(2)(ii)(A)(

- 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.[48]
- 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.[49]
- Make a reasonable determination of the likelihood that each identified threat would exploit the identified vulnerabilities.[50] 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.[5152] 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]

[48] Proposed 45 CFR 164.308(a)(2)(ii)(A)(*3*).
[49] Proposed 45 CFR 164.308(a)(2)(ii)(A)(*4*).
[50] Proposed 45 CFR 164.308(a)(2)(ii)(A)(*5*).
[51] Proposed 45 CFR 164.308(a)(2)(ii)(A)(*6*).
[52]).
Proposed 45 CFR 164.308(a)(2)(ii)(A)(

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

---

488 *8*).

Proposed 45 CFR 164.308(a)(2)(ii)(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.[53]

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 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.[54] They include:

---

[53] *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.

[54] *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.

- 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

Department of Health and Human Services (Feb. 16, 2024), https://www.hhs.gov/hipaa/forprofessionals/security/guidance/index.html?language=es.

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.[55] 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

[55] *See* "Defending Against Common Cyber-Attacks," *supra* note 396.

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,[56] 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 poses to ePHI is important to ensuring that ePHI is protected.[57]

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).[58]

Patches can be applied to software and firmware on all types of devices—telephones,

---

[56] 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.

[57] *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-2018newsletter-software-patches.pdf.

[58] *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/forprofessionals/security/guidance/cybersecurity-newsletter-fall-2021/index.html.

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.[59] Enterprise patch management is the process of identifying, prioritizing, acquiring, installing, and verifying the installation of patches, updates, and upgrades throughout an organization.[60] 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

---

[59] *See* "Guidance on Software Vulnerabilities and Patching," *supra* note 493.
[60] *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.

(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,[61] 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

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

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 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.[62]

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

[62] "Cybersecurity Performance Goals," *supra* note 18. [500]
See proposed 45 CFR 164.308(a)(2).

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.[63]

The Department previously issued guidance on risk management, including links to NIST resources, that is consistent with what we propose in this NPRM.[64] We encourage regulated entities to refer to similar NIST guidance for descriptions of risk management activities.[65] 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.[66] 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.[67]

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,

---

[63] "Cybersecurity Performance Goals," *supra* note 18.
[64] *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.
[65] *See* "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide," *supra* note 461.
[66] *See id*. at 18.
[67] *See id*. at 25.

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.[68] 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.[69]

As stated by NIST, "the documentation and retention of risk assessment and risk management activities" is "important for future risk management efforts."[70] 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."[71] 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 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.

---

[68] *Id.*

[69] *See* proposed 45 CFR 164.306(d) and 164.316(b)(1).

[70] *See* "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide," *supra* note 461, p. 27.

[71] *See id*. at 31. [510]

See id.

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.[72] 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.[73] 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

[72] "The 2024 Study on Cyber Insecurity in Health Care: The Cost and Impact on Patient Safety and Care," *supra* note 143, p. 7.

[73] *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/forprofessionals/security/guidance/cybersecurity-newsletter-october-2023/index.html#ftn10.

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.[74] 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.[75] 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.[76]

---

[74] 68 FR 8334, 8347 (Feb. 20, 2003).
[75] 65 FR 82462, 82747 (Dec. 28, 2000). [515]
68 FR 8334, 8347 (Feb. 20, 2003).
[76] 65 FR 82462, 82562 (Dec. 28, 2000).

- Requiring workforce members to affirmatively acknowledge that a violation of the organization's HIPAA policies or procedures may result in sanctions.[77]
- 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.[78]
- Creating sanctions that are "appropriate to the nature of the violation."[79]
- 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]."[80]
- Creating sanctions that "range from a warning to termination."[81]
- Providing examples "of potential violations of policy and procedures."[82]

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.[83] 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.

---

[77] *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.

[78] Records of sanction activity should be retained for at least six years. *See* 45 CFR 164.316 and 164.530(e)(2).

[79] *See* 65 FR 82462, 82562 (Dec. 28, 2000).

[80] *Id.*

[81] *Id.*

[82] *See* "Security Standards: Administrative Safeguards," *supra* note 517.

[83] *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,[84] enables a regulated entity to determine if any ePHI has been used or disclosed in an inappropriate manner.[85] The procedures should be customized to meet the regulated entity's risk management strategy and consider the capabilities of all information systems with ePHI.[86] These activities should also promote continual awareness of any information system activity that could suggest a security incident.[87]

Detecting and preventing data leakage initiated by malicious authorized users is a significant challenge.[88] 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.[89] 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.[90] 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

---

[84] 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.
[85] *See* "Security Standards: Administrative Safeguards," *supra* note 517, p. 5-6.
[86] *See id*. at 6.
[87] *Id.*
[88] *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/forprofessionals/security/guidance/cybersecurity-newsletter-summer-2019/index.html.
[89] *Id.*
[90] *Id.*

reports are important security measures that can assist in detecting and identifying suspicious activity or unusual patterns of data access.[91]

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.[92] 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.[93] They also must activate the necessary review processes and maintain auditing and logging activity.[94]

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.[95] 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

---

[91] *Id.*

[92] *See* "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide," *supra* note 461, p. 33.

[93] *See id*. at 34.

[94] *See id*.

[95] *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.

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.[96] 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.[97] 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.[98]

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.[99] 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

---

[96] *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://prodwwwhhsgov.cloud.hhs.gov/about/news/2024/07/01/hhs-office-civil-rights-settles-hipaa-security-rule-failures950000.html.
[97] *See* "Montefiore Medical Center," *supra* note 248.
[98] *See* 45 CFR 164.308(a)(1)(ii)(D).
[99] *See* "Doctors' Management Services, Inc.," *supra* note 246. [540]
Id.

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 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.[100] 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.

---

[100] *See* proposed 45 CFR 164.308(a)(12)(ii)(B).

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,[101] 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?

---

[101] *See* "Security Standards: Administrative Safeguards," *supra* note 517, p. 7.

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.[102] 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 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.[103][104] OCR's

---

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

[103] *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-

[104] T08:51/https://www.hhs.gov/about/news/2020/10/30/city-health-department-failed-terminate-formeremployees-access-protected-health-information.html.

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.[105] 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).[106] 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.[107] 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.[108] 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

[105] *See* "Security Standards: Administrative Safeguards," *supra* note 517, p. 8-11.
[106] *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.
[107] *See* 45 CFR 164.502(b) and 164.514(d).
[108] *See* "Security Standards: Administrative Safeguards," *supra* note 517, p. 9.

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.[109] 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,

[109] *See* "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide," *supra* note 461. [550] *See id.* at 36.

but it is still liable for ensuring that workforce members only have access to ePHI that they need to perform their assigned functions.[110]

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.[111] 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.[112] 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.[113] 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 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.[114]

---

[110] *See* proposed 45 CFR 164.308(a)(9)(i).
[111] *See* "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide," *supra* note 461, p. 36.
[112] *See id*.
[113] *See* "Security Standards: Administrative Safeguards," *supra* note 517, p. 10.
[114] *See* "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide," *supra* note 461, p. 37.

We issued guidance in 2017 addressing termination procedures.[115] 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.[116]

Guidance that we issued in 2019 further explains that "security is a dynamic process."[117] 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.[118] As described in other HHS guidance, these procedures should also

---

[115] *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/novembercybersecurity-newsletter-11292017.pdf.
[116] *See* "Managing Malicious Insider Threats," *supra* note 528.
[117] *Id*.
[118] *See* 45 CFR 164.308(a)(4)(ii)(C).

address the complexity of the organization and the sophistication of its relevant electronic information systems.[119]

NIST guidance provides additional descriptions of key activities and sample questions for regulated entities to consider when implementing this standard and associated implementation specifications.[120] 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

---

[119] *See* "Security Standards: Administrative Safeguards," *supra* note 517, p. 10-11.
[120] *See* "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide," *supra* note 461.

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.[121] 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, 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

[121] *See* proposed 45 CFR 164.308(a)(9)(ii)(A).
[563] *See* proposed 45 CFR 164.308(a)(9)(ii)(B).

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.[122] 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.[123]

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

[122] *See* proposed 45 CFR 164.308(a)(9)(ii)(E).
[123] "Cybersecurity Performance Goals," *supra* note 18.

entities with a need for access is a basic tenet of security.[124] 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.[125] 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.[126]

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.[127][128][129][130] This failure also enabled other employees to inappropriately access the ePHI of a celebrity.[131]

---

[124] *See* "Security Standards: Administrative Safeguards," *supra* note 517, p.11.
[125] *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/complianceenforcement/agreements/banner-health-ra-cap/index.html; "Montefiore Medical Center," *supra* note 248.
[126] *See* 45 CFR 164.502(b) and 164.514(d).
[127] *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-
[128] T08:51/https://www.hhs.gov/about/news/2019/10/23/ocr-imposes-a-2.15-million-civil-money-penalty-againstjhs-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-
[129] T08:51/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-
[130] T08:51/https://www.hhs.gov/sites/default/files/jackson-health-system-notice-of-final-determination_508.pdf.
[131] *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-arizonahospital-system.html.

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.[132] This necessarily includes its relevant electronic information systems. First, the regulated entity must determine whether any of its components constitute a health care clearinghouse under the Security Rule.[133] If no health care clearinghouse

[132] *See* "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide," *supra* note 461.
[133] 45 CFR 160.103 (definition of "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

---

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.

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,[134] 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[135] 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.

---

[134] 45 CFR 164.308(a)(4)(ii)(C).

[576] 45 CFR 164.308(a)(4)(ii)(B).

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

- 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,[136] 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

[136] *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).

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 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.[137] 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

[137] *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/july2017-ocr-cyber-newsletter.pdf.

workforce members on security issues, given the risks and threats to their enterprises. Computerbased 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.[138] NIST has also provided detailed guidance for developing and implementing workforce training programs.[139] 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.[140] 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

---

[138] *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.
[139] *See* "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide," *supra* note 461.
[140] *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.

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.[141] 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.[142]

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.[143]
- Guarding against, detecting, and reporting suspected or known security incidents, including but not limited to malicious software and social engineering.[144]

[141] "Cybersecurity Performance Goals," *supra* note 18.
[142] *Id*.
[143] Proposed 45 CFR 164.308(a)(11)(ii)(A)(*1*).
[144] Proposed 45 CFR 164.308(a)(11)(ii)(A)(*2*).

- 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.[145] 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 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[146] 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.[147] 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.[148] We also propose to require that the regulated entity provide such training.[149] For example, if the entity implements a new EHR system, it

[145] 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.
[146] 45 CFR 164.308(a)(5)(ii)(A).
[147] Proposed 45 CFR 164.308(a)(11)(ii)(B)(*1*).
[148] Proposed 45 CFR 164.308(a)(11)(ii)(B)(*2*).
[149] Proposed 45 CFR 164.308(a)(11)(ii)(B)(*3*).

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.[150] 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

[150] *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/forprofessionals/security/guidance/cybersecurity-newsletter-october-2022/index.html.

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.[151]

NIST also offers guidance for addressing security incidents.[152] 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.[153] 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."[154] "Respond" supports the ability of the regulated entity "to contain the effects of cybersecurity

---

[151] *Id*.

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

[153] *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/privacyframework/nist-sp-800-61.

[154] "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*.

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.[155]

Internal reporting is an essential component of security incident procedures.[156] Plans and procedures for 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.

---

[155] Proposed 45 CFR 164.308(a)(12)(ii)(A)(*1*).

[156] *See, e.g.*, Joint Task Force, "Security and Privacy Controls for Information Systems and 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.

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).[157]

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.[158] 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.[159]

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

---

[157] "Cybersecurity Performance Goals," *supra* note 18; *see also* proposed 45 CFR 164.314(a)(2)(i)(C).
[158] "Cybersecurity Performance Goals," *supra* note 18.
[159] *Id*.

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.[160] 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.[161]

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.[162] 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

---

[160] *See* "Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology," *supra* note 597.

[161] *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.

[162] *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-newslettercontingency-planning.pdf.

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.[163] 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.[164] Unfortunately, many regulated entities have not implemented the required 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.[165] 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

---

[163] *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/.

[164] *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.

[165] *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://prodwwwhhsgov.cloud.hhs.gov/about/news/2024/07/01/hhs-office-civil-rights-settles-hipaa-security-rule-failures950000.html.

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.[166]

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

[166] *See* "Security Standards: Administrative Safeguards," *supra* note 517, p. 22.

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.[167]

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.

[167] *See* proposed 45 CFR 164.308(a)(13)(ii)(A).

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.[168] 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."[169] 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.[170][171]

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.[172] NIST guidance explains that regulated entities, are permitted to include more stringent cybersecurity measures in

---

[168] *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.

[169] *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-updateof-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf.

[170] We believe that health plans that are subject to HIPAA and to the Employee Retirement Income Security Act of

[171] 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/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-release2024-01.

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

business associate agreements than those required by the Security Rule.[173] 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.[174] 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

---

[173] *Id.* at 54.
[617] *Id.*
[174] *See* 45 CFR 164.306(a)(1).
[619] *See* 45 CFR 164.308(b).

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[175] in addition to obtaining satisfactory assurances that its business associate would comply with the Security Rule.[176] 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.[177] 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.[178] Additionally, we propose that the verification include a written analysis of the business associate's relevant electronic information systems.[179] 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.[180] 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.[181] The proposal would permit the parties to determine the appropriate person to

[175] *See* proposed 45 CFR 164.308(b)(1)(i) and (ii).
[176] *Id.*
[177] *See* proposed 45 CFR 164.308(b)(2)(ii).
[178] *Id.*
[179] Proposed 45 CFR 164.308(b)(2)(ii)(A).
[180] *Id.*
[181] Proposed 45 CFR 164.308(b)(2)(ii)(B).

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.[182] This CPG calls for regulated entities to identify, assess, and mitigate risks to ePHI used by or disclosed to business associates.[183]

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.[184] 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.[185]

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.

---

[182] "Cybersecurity Performance Goals," *supra* note 18; *see also* proposed 45 CFR 164.308(b)(2)(i).
[183] "Cybersecurity Performance Goals," *supra* note 18.
[184] Proposed 45 CFR 164.308(b)(3)(i).
[185] 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.