799 9th Street NW
Suite 210
Washington, DC 20001

T (202) 354-2600
vizientinc.com

Vizient Office of Public Policy and Government Relations

Proposed Rule: HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information

February 5, 2025

Background & Summary

On January 6, the Office for Civil Rights (OCR), Office of the Secretary within the Department of Health and Human Services (HHS) issued a Proposed Rule to modify the Security Standards for the Protection of Electronic Protected Health Information ("Security Rule") under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act) (hereinafter, "Proposed Rule"). The Security Rule was originally finalized in 2003[1] and adopted standards for regulated entities (i.e., covered entities and business associates) to ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit; protect against reasonably anticipated threats or hazards to the security or integrity of the information; and ensure compliance by their workforce. The Security Rule was most recently revised in 2013.[2]

The modifications in the Proposed Rule revise existing Security Rule standards to address an increased reliance on secure computer and network technologies, increases in breaches and cyberattacks, and inconsistent compliance with the requirements of the Security Rule by regulated entities. The Proposed Rule includes new requirements for regulated entities including ensuring development and maintenance of written documentation of all Security Rule policies, procedures, plans, and analyses; strengthening requirements for planning for contingencies and responding to security incidents; conducting a Security Rule compliance audit at least once every 12 months; and reviewing and testing the effectiveness of certain security measures at least once every 12 months.

Comments on the Proposed Rule are due on March 7, 2025. Vizient looks forward to working with our provider clients to help inform our letter to the agency.

Key Takeaways

Definitions

To better account for the increased reliance on the use of technology in the health care environment, OCR proposes adding and modifying regulatory definitions to clarify how regulated entities should apply the standards and implementation specifications to the Security Rule. OCR proposes adding 10 new definitions and modifying 15 existing definitions.[3] Below is additional information about certain proposed new and modified definitions.

[1] 45 CFR 160 and 45 CFR 164
[2] In 2013, the Department issued the final rule "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health [HITECH] Act and the Genetic Information Nondiscrimination Act, and Other Modifications to the HIPAA Rules" ("2013 Omnibus Rule"), which implemented applicable provisions of the HITECH Act to strengthen security protections for individuals' health information maintained in EHRs.
[3] View a full list of all proposals regarding definitions starting on page 76 of the Proposed Rule.

New Definitions

- “Deploy” and “Implement”: OCR believes it is necessary to add definitions that distinguish between implementation of the administrative and technical safeguards by separately describing how regulated entities can comply with requirements to implement technical safeguards and install technical solutions.
  - Deploy: OCR proposes to define the term “deploy” to identify a specific type of “implementation” to help better describe the compliance obligations for implementation specifications related to the use of technology for securing the confidentiality, integrity, or availability of ePHI.[4] The proposed definition of deploy requires a regulated entity to ensure that technology is in place, configured for use, and in use and operational throughout the regulated entity.[5]
  - Implement: OCR proposes to define “implement” to clarify that a safeguard must be put into place and be in effect throughout the enterprise, as opposed to only some components of a regulated entity’s relevant information systems (e.g., some laptops or servers) or applied to a subset of ePHI.[6] Additionally, through the proposed definition of implement, OCR aims to clarify what it means to configure and put technology, technical controls, and related policies and procedures into effect and be in use, operational, and function as expected throughout the regulated entity’s enterprise (i.e., deploy) as compared to putting into place and making effective administrative or physical safeguards.[7]
- “Electronic information system”: The current Security Rule includes explicit requirements for regulated entities to protect electronic information systems but does not explicitly define “electronic information system”. Rather, only “information system” is defined.[8] To better distinguish an “electronic information system” from the broader category of an “information system,” OCR proposes to define electronic information system as an interconnected set of electronic information resources under the same direct management control that shares common functionality. An electronic information system generally includes technology assets, such as hardware, software, electronic media, information, and data.[9]
- “Multi-factor Authentication” (MFA): Due to concerns about the adequacy of approaches regulated entities use to identify users and authenticate users to the system, OCR proposes to define MFA to provide a specific level of authentication for access to relevant electronic

[4] OCR is concerned, based on its investigations and compliance reviews, that some regulated entities may interpret the regulatory requirement to implement technical policies and procedures to mean that a regulated entity is only required to establish written policies and procedures about technical requirements, but need not then apply effective, automated technical policies and procedures to all ePHI throughout the regulated entity’s enterprise.

[5] OCR’s proposed use of the term “deploy” helps illustrate its purpose in clarifying that policies and procedures, while necessary, are insufficient to meet requirements for technical safeguards. For example, the Department is proposing new implementation specifications under the access control standard that would require a regulated entity to deploy technical controls for relevant electronic information systems so that the system is configured and applied to limit access to only users and technology assets that have been granted access rights. In this case, the technical controls must not only be configured for use, but they also must be applied to and in effect in all ePHI and relevant electronic information systems

[6] OCR is concerned, based on its investigations and compliance reviews, that some regulated entities may interpret the regulatory requirement to implement technical policies and procedures to mean that a regulated entity is only required to establish written policies and procedures about technical requirements, but need not then apply effective, automated technical policies and procedures to all ePHI throughout the regulated entity’s enterprise.

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

[8] OCR proposes that “Information system” means an interconnected set of information resources under the same direct management control that shares common functionality. An information system generally includes hardware, software, information, data, communications, and people.

[9] This proposal limits the definition to an interconnected set of electronic information resources under the same direct management control that shares common functionality.

information systems. Specifically, OCR proposes that MFA means "authentication of the user's identity through verification of at least two of the following three categories: (1) Information known by the user, including but not limited to a password or personal identification number (PIN); (2) Item possessed by the user, including but not limited to a token or a smart identification card; (3) Personal characteristic of the user, including but not limited to fingerprint, facial recognition, gait, typing cadence, or other biometric or behavioral characteristics."

- "Relevant electronic information system": To clarify the scope of regulated entities' compliance obligations, OCR proposes to define "relevant electronic information system" as an electronic information system that creates, receives, maintains, or transmits ePHI or that otherwise affects the confidentiality, integrity, or availability of ePHI.

Modified Definitions

- "Authentication": To modernize the definition of authentication and reflect cybersecurity best practices, OCR proposes to broaden the definition of authentication to mean corroboration that either a person or technology asset is the one they are claiming to be. As a result of the proposal, OCR notes that not only must an individual be an authenticated user, but the application must also be authenticated (e.g., a covered entity's software can verify the application is what it claims to be).
- "Availability": Although not intended, OCR believes the current definition of availability could be read to limit who may access data or information regulated under the Security Rule to just an authorized person.[10] OCR proposes to clarify the definition to include "technology asset". Specifically, OCR proposes "Availability means the property that data or information is accessible and useable upon demand by an authorized person or technology asset."[11]
- "Electronic Media": Given the range of new and emerging technologies that regulated entities may use, particularly those for remote communications (e.g., smart phone application, voice over internet technologies, technologies that transcribe a telehealth session, messaging serves that electronically store audio messages), OCR proposes to broaden the scope of electronic media.[12] Specifically, OCR proposes to clarify that electronic media includes media on which data may be maintained or processed. In addition, OCR proposes to provide a non-exhaustive list of examples of electronic storage materials, including "any other form of digital memory or storage" on which data may be recorded, maintained or processed.
- "Malicious software": OCR proposes to replace the current definition of malicious software with one that would be consistent with how cybersecurity experts currently define the term. The proposed definition of malicious software is, "software or firmware intended to perform an unauthorized action or activity that will have adverse impact on an electronic information system and/or the confidentiality, integrity, or availability of electronic protected health information."
- "Security incident": According to OCR, the existing definition does not make clear that a security incident may result from two types of behaviors. To provide greater clarity, OCR proposes to modify the definition to delineate the two separate categories of security incidents (i.e., "The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information in an information system" and "The attempted or successful unauthorized interference with system operations in an information system").

[10] Availability is currently defined in the Security Rule as "the property that data or information is accessible and usable upon demand by an authorized person".

[11] OCR also proposes to define "technology asset" to mean "the components of an electronic information system, including but not limited to hardware, software, electronic media, information, and data."

[12] To clarify, OCR proposes to update the definition of electronic media at 45 CFR 160.103 (General Administrative Requirements).

Safeguards and Other Requirements

Currently regulated entities must meet Security Standards, Administrative Safeguards, Physical Safeguards, Technical Safeguards, Organizational Requirements and Documentation Requirements in the Security Rule. Within each of these categories, regulations provide additional details for compliance, such as general rules and standards (standards are further detailed through implementation specifications). OCR proposes various updates to the requirements and safeguards that regulated entities must meet, with several key examples provided below.

Security Standards: General Rules

General Requirements

In the Proposed Rule, OCR states the agency is concerned that regulated entities are misinterpreting the requirements of the current Security Rule by applying the rule only to some ePHI, rather than all ePHI.[13] Therefore, among other changes, OCR proposes to modify the general requirements of the portion of the regulation on security standards to require each regulated entity to apply the requirements of the Security Rule to protect all the ePHI they create, receive, maintain, or transmit, instead of only to the security or integrity of ePHI.[14]

OCR also proposes to require each regulated entity to protect against any reasonably anticipated threats or hazards to the confidentiality, integrity, or availability of all ePHI, instead of to the security or integrity of ePHI.

Additionally, the Proposed Rule also requires each regulated entity to ensure that its workforce complies not only with the Security Rule, but also all administrative, physical, and technical safeguards implemented in accordance with this subpart.

Flexibility of Approach

To acknowledge the rapid evolution of technology and increasing security threats, OCR proposes to clarify that regulated entities are required to apply reasonable and appropriate security measures to implement the standards and specifications of the Security Rule. OCR indicates that a regulated entity is required to implement the standards and implementation specifications and must adopt reasonable and appropriate security measures that allow the entity to achieve such implementation.

OCR also proposes adding a new element to the list of factors that regulated entities must consider when deciding whether a particular security measure (e.g., a technical control) is reasonable and appropriate. The new element to be added to the list of factors is that a regulated

[13] Specifically, OCR is concerned that regulated entities are misinterpreting the requirements of the current Security Rule by applying the rule only to some ePHI, rather than all ePHI which could lead to inadequate protection of ePHI and relevant electronic information systems. OCR is also concerned that regulated entities have focused their attention on the cost of security measures, rather than considering the reasonableness and appropriateness of security measures, including the probability and criticality of potential risks to ePHI.

[14] OCR believes that this proposal would stress to regulated entities that each and every covered entity and business associate would be responsible for ensuring it meets Security Rule requirements with respect to all ePHI. OCR believes this proposed change would also help address issues raised by current interpretations of the Security Rule that suggest that its plain wording may not require regulated entities to fully implement each security measure to protect all ePHI. The proposed language would clarify that a security measure must be implemented such that it protects the security of all ePHI and all information systems that affect the confidentiality, integrity, and availability of ePHI.

entity must consider the effectiveness of the security measure in supporting the resiliency of the regulated entity. A regulated entity would be required to consider this factor, in addition to the existing factors, for example, when choosing a specific encryption solution that allows the entity to meet the proposed requirement to encrypt ePHI, which will help prevent an unauthorized user from accessing the entity's ePHI.

Additionally, OCR proposes a new requirement for regulated entities where they must evaluate the effectiveness of the security measures they choose to ensure the regulated entity can continue its operations and recover quickly during or after a security incident.[15]

Standards and Implementation Specifications

In prior rulemaking, to provide greater flexibility, OCR introduced the concept of "addressable" implementation specifications, which is distinguished from "required" implementation specifications.[16] However, OCR is concerned that many regulated entities are not complying by misinterpreting the difference between required and addressable implementation specifications and are treating addressable implementation specifications as optional. To provide greater clarity, OCR proposes to eliminate the distinction between "addressable" and "required." OCR also indicates that the Security Rule sets a floor for cybersecurity protections and flexibility in compliance approaches still exists.[17]

Request for Comments on Security Standards: General Rules

OCR requests comments on the Security Standard proposals, including any benefits, drawbacks, or unintended consequences. OCR also requests comments on the following considerations:

- **Whether OCR should include other factors for regulated entities to consider when selecting the security measures that they will implement to meet the requirements of the Security Rule. If so, please explain.**
- **Whether the new proposed factor (i.e., a regulated entity is to consider the effectiveness of the security measure in supporting the regulated entity's resiliency) would help regulated entities identify reasonable and appropriate security measures.**
- **Whether OCR's proposals sufficiently clarify that a regulated entity is expected to modify its security measures in response to changes in the environment in which health care is provided, including, but not limited to, the adoption of new technology, the evolution of existing technology, and the emergence of new threats.**

[15] OCR proposes this new requirement to better enable regulated entities to ensure the confidentiality, integrity, and availability of all ePHI that they create, receive, maintain, or transmit. The general rules require regulated entities to not only prevent threats and hazards to the confidentiality and integrity of ePHI, but also to ensure the availability of ePHI, even during a security incident that has the potential to severely hinder the ability of a regulated entity to provide health care or to bring it to a standstill.

[16] In the 2003 Final Rule, the Department introduced the concept of "addressable" implementation specifications, which it distinguished from "required" implementation specifications. The goal was to provide covered entities with even more flexibility. While none of the implementation specifications were optional, designating some of the implementation specifications as addressable provided each covered entity with the ability to determine whether certain implementation specifications were reasonable and appropriate safeguards for that entity, based on its risk analysis, risk mitigation strategy, previously implemented security measures, and the cost of implementation. However, over time stakeholders asked for removal of the "addressable" designation from the Security Rule because it leads to ambiguity in the rule's application.

[17] For example, a small or rural health care provider must implement a solution that ensures the protection of ePHI in the manner required by the Security Rule, but the specific solution that it chooses would reflect consideration of its specific circumstances, including available resources. In some cases, a small or rural health care provider might opt to implement a cloud-based EHR or other software solution that could reduce the health care provider's need to separately invest in data storage, backup systems, and IT personnel.

Administrative Safeguards

The standards and implementation specifications found in the Administrative Safeguards section of the Security Rule refer to administrative functions (e.g., standards, policies and procedures) that must be in place for the management and execution of security measures.[18] This also includes the administrative safeguards that apply to the relationships between regulated entities (i.e., covered entities and business associates). OCR observed inadequacies in compliance with current administrative safeguards and is concerned that some covered entities entrusted ePHI to business associates that are not employing appropriate safeguards. As a result, OCR proposes to update Administrative Safeguards standards,[19] some of which are detailed below.

Standard: Technology Asset Inventory

OCR proposes a standard for Technology Asset Inventory that requires a regulated entity to conduct and maintain an accurate written technology asset inventory and a network map[20] of its electronic information systems and all technology assets that may affect the confidentiality, integrity, or availability of ePHI. The proposed standard would be accompanied by three implementation specifications, which provide detail on how to meet the standard, for the written technology inventory[21], network map[22] and maintenance.[23]

Standard: Risk Analysis

OCR learned through its compliance and enforcement activities that regulated entities often do not perform compliant risk analyses, which is currently an implementation specification under a standard within the Administrative Safeguards section of the regulation. As a result, OCR proposes to elevate the implementation specification to conduct a risk analysis to a standard. Under the proposed standard, 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. Also, a regulated entity would be required to review, verify, and update the written assessment on an ongoing basis, but 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.

Standard: Patch Management

OCR proposes a new standard for patch management 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.

[18] A full list of standards can be found on page 114 of the Proposed Rule

[19] OCR proposes the following standards, each of which are generally accompanied by implementation specifications: Technology asset inventory; Risk analysis; Evaluation; Patch Management; Risk management; Sanction policy; Information system activity review; Assigned security responsibility (note: there are not implementation specifications); Workforce security; Information access management; Security awareness training; Security incident procedures; Contingency plan; Compliance audit; Business associate contracts and other arrangements; and Delegation to business associate)

[20] A regulated entity's network map would reflect the location of technology assets (e.g., physically located at the regulated entity's worksite, accessed through the cloud).

[21] The proposed written inventory specification requires regulated entities 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. It would also be required to include the identification, version, person accountable for, and location of each of the assets or information system component.

[22] The proposed implementation specification for network map 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.

[23] The proposed implementation specification for maintenance requires a regulated entity 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.

Standard: Information System Activity Review

OCR learned through its compliance and enforcement activities that regulated entities would benefit from additional detail on compliance expectations for information activity review, which is currently an implementation specification under a standard within the Administrative Safeguards section of the regulation. As a result, OCR proposes to advance the existing implementation specification for information system activity review to a standard where a regulated entity ensures that only appropriate users access ePHI and will respond quickly to any suspicious activity in its relevant electronic information systems.

Standard: Security Incident Procedures

In the Proposed Rule, OCR states that their enforcement experience indicates that many regulated entities have not met the existing standard for security incidents. As a result, OCR proposes a new standard for regulated entities to establish a written security incident response plan and procedures detailing how workforce members are to report suspected or known security incidents and how the regulated entity will respond to suspected or known security incidents.

Among other changes, OCR proposes to modify existing 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 because additional specificity is needed regarding their obligations and liability for incident response. The Proposed Rule does not dictate the form, format, or content of these security incident reports. Rather, the regulated entity would need 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. Also, the regulated entity would be required to implement written procedures for testing and revising the security incident response plans and then, using those written procedures, review and test its security incident response plans at least once every 12 months and document the test results.

Standard: Business Associate Contracts and Other Arrangements

The Security Rule does not currently 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 ePHI. OCR indicates that 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, OCR proposes several modifications to the Security Rule to provide greater assurance that business associates and their subcontractors are protecting ePHI. OCR proposes to add a requirement for the regulated entity to obtain written verification from their business associate confirming that the business associate has deployed the required technical safeguards[24].

The proposed written verification must include a written analysis of the business associate’s relevant electronic information systems. The written analysis is 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. This is to verify the business associate’s compliance with each standard and implementation specification in the Security Rule. OCR also proposes 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

[24] See 45 CFR 164.306(a)(1) and 45 CFR 164.308(b)

that the analysis has been performed and is accurate. This person may be a member of the covered entity's or business associate's workforce or an external party.

OCR proposes to require that the regulated entity obtain this written verification (which is to include a written analysis of the business associate's relevant electronic information systems) documenting the business associate's deployment of the required technical safeguards at least once every 12 months.

Standard: Delegation To Business Associate

The Proposed Rule states that regulated entities are often not aware that they are responsible for implementing requirements of the Security Rule, even when the functions of designated security official have been delegated to a business associate. Therefore, OCR proposes a new standard that indicates that a regulated entity may permit a business associate to serve as its designated security official. However, the proposed standard makes clear that should the designated security official's function be delegated to a business associate then, the delegating regulated entity remains liable for compliance with the Security Rule.

Request for Comments on Administrative Safeguards

OCR request comments on these Administrative Safeguard proposals and also on the following additional considerations:

- **Whether there are any special considerations for business associates and business associate agreements that OCR should be aware of with respect to administrative safeguards.**
- **Whether there are any requirements for business associates and business associate agreements that OCR should include in administrative safeguards that it did not propose.**
- **Whether OCR 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, what are the appropriate circumstances of and the appropriate amount of time for such notification.**
- **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.**
- **Whether OCR 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.**

Physical Safeguards

As noted in the Proposed Rule, physical safeguards encompass the physical measures, and related policies and procedures, to protect relevant electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion. Based on OCR's enforcement experience, breaches occur because of absent or insufficient physical safeguards (e.g., devices stored in unlocked rooms and a lack of alarm systems; loss of unencrypted flash drive and unencrypted laptop). To address these concerns, OCR proposes several modifications to existing physical safeguards requirements, including clarifying that the Security Rule requires that physical safeguards be applied to all ePHI in the possession of the regulated entity, that is, throughout the regulated entity's facilities. Also, OCR proposes to broaden the requirements so that a regulated entity implements physical safeguards for documentation requirements.[25] OCR also proposes changes to the following standards: Facility access controls; Workstation use; Workstation security; and Technology asset controls which are further detailed in the in the Proposed Rule (pg. 197-204).

Technical Safeguards

Current Technical Safeguards standards provide requirements concerning the implementation of technology and technical policies and procedures to protect the confidentiality, integrity, and availability of ePHI and related information systems. Based on OCR's investigations, compliance reviews, news reports and published studies, OCR believes many regulated entities have failed to implement adequate technical controls (e.g., failure to monitor activity in a health system's information systems that was insufficient to protect against a cyberattack; failure to implement an authentication process to safeguard ePHI; failure to encrypt ePHI; lack of device and media controls; failure to implement reasonable and appropriate policies and procedure to comply with the standards). As a result, OCR proposes additions and modifications to the existing standards.[26] OCR proposes to modify the Authentication standard to replace the requirement for a regulated entity to implement procedures with a requirement to deploy technical controls. Also, OCR proposes implementation specifications which aim to eliminate the use of default passwords and to require a regulated entity to deploy MFA. OCR indicates that it requires a regulated entity to deploy MFA to all technology assets in its relevant electronic information systems to verify that the person seeking access to its relevant electronic information system is the user that the person claims to be. Further, OCR indicates that a regulated entity should deploy MFA to all technology assets in its relevant electronic information systems in a manner consistent with its risk analysis. In the Proposed Rule (pg. 243-246), OCR also proposes three exceptions related to MFA.

In addition, and among several other proposed changes, OCR proposes to impose network segmentation requirements. Specifically, a regulated entity would be required to deploy technical controls to ensure that the covered entity's or business associate's relevant electronic information systems are segmented in a reasonable and appropriate manner.

Organizational Requirements

Currently, regulated entities are required to establish, and implement as needed, a contingency plan that includes the policies and procedures for responding to an emergency or other occurrence that damages systems that contain ePHI. In the Proposed Rule, OCR states that there has been an increased risk in the number and types of emergencies or other occurrences (e.g., extreme weather events, breaches of unsecured PHI reported to the Department) that cause damage to systems that contain ePHI and may require a regulated entity to activate its contingency plan. Additionally, OCR noted in the Proposed Rule that business associates have not been promptly notifying covered entities about security incidents affecting their ability to access ePHI or transmit ePHI.

To address these risk trends and deficiencies in protections, OCR proposes to add an implementation specification requiring a business associate agreement to include a provision for a business associate to report to the covered entity activation of its contingency plan that would be

[25] Specifically, OCR proposes to expand this section to expressly require a regulated entity to implement physical safeguards in accordance with not only 45 CFR 164.306, but also 45 CFR 164.316 to connect the overarching documentation requirements.
[26] OCR proposes changes to the following standards: Access Control; Encrypton and Decryption; Configuration Management; Audit Trail and System Log Controls; Authentication; Transmission Security; Vulnerability Management; Data Backup and Recovery; and Information Systems Backup and Recovery.

required without unreasonable delay[27], but no later than 24 hours after activation[28]. However, OCR clarifies that this proposal would not require reporting on the cause of the contingency plan activation. Instead, OCR indicates that reporting would be solely on the fact that the business associate has activated the contingency plan. The proposal would only require that the business associate notify the covered entity of its activation of the contingency plan. OCR does not include any specific requirements with respect to the form, content, or manner of the notice. Instead, the agency proposes to permit the covered entity and business associate to negotiate these terms and include them in their business associate agreement as desired.

Documentation Requirements

In the Proposed Rule, OCR outlines current issues that it aims to address related to documentation requirements, including how regulated entities must implement, maintain, and document implementation of all security measures and how to ensure regulated entities commit to writing the security measures required by the Security Rule. Further, OCR notes that regulated entities may not be periodically reviewing and updating their documentation as currently required by the Security Rule when they modify their security measures in response to environmental or operational changes affecting the security of their ePHI.

As a result, OCR proposes additional documentation requirements, including renaming the section in which documentation requirements are outlined from “policies and procedures and documentation requirements” to “documentation requirements”. In addition, among other changes, OCR proposes that a regulated entity document the policies and procedures it has implemented to comply with the Security Rule. Further, as part of that documentation, regulated entities would be required to explain how their policies and procedures considered the factors provided in the Security Standards.[29] OCR also proposes to clarify that all required written documentation may be in electronic form. In addition, OCR proposes that a regulated entity would be required to update its documentation at least once every 12 months and within a reasonable and appropriate time after a security measure is modified.

Compliance Period for Regulated Entities

Currently, regulated entities must comply with applicable new or modified standards or implementation specifications no later than 180 days from the effective date of any such change.[30] OCR attests that most of the modifications in the Proposed Rule would provide regulated entities with greater clarity and specificity regarding how to fulfill their obligations and the agency does not believe that the Proposed Rule would pose unique implementation challenges that would justify an extended compliance period.

However, to help reduce administrative burdens OCR proposes to add a provision for a longer transition period to modify business associate agreements, if needed. Specifically, OCR proposes to allow regulated entities to continue to operate under certain existing business associate

[27] This proposal would align with the enhanced Cybersecurity Performance Goals (CPG) for Third Party Incident Reporting because this proposal would require a business associate to both report to a covered entity or another business associate activation of its contingency plan within 24 hours of such activation and report known or suspected security incidents.
[28] The proposed requirement to provide notice without unreasonable delay, but no later than 24 hours after a contingency plan is activated, would also apply when a business associate that is a governmental entity enters into an arrangement with a covered entity that is also a governmental entity and also when a business associate enters into a business associate agreement with a subcontractor
[29] Specifically, the factors provided at 45 CFR 164.306(b)
[30] 42 U.S.C. 1320d–4(b)(2)

agreements or other written arrangements until the earlier of: (1) the date such contract or other arrangement either is renewed on or after the compliance date of the final rule; or (2) a year after the effective date of the final rule. The additional transition period would be available to regulated entities if both of the following conditions are met: (1) prior to the publication date of the final rule, the covered entity or business associate had an existing business associate agreement or other written arrangement with a business associate or subcontractor, respectively, that complied with the Security Rule prior to the effective date of a final rule revising the Security Rule; and (2) such contract or arrangement would not be renewed or modified between the effective date and the compliance date of the final rule. **OCR seeks comments on the proposed compliance period and transition period.**

New and Emerging Technologies Request for Information

The Proposed Rule states that as technology progresses and its use increases, regulated entities must consider how to secure ePHI from security breaches. The Proposed Rule lists examples of new technologies, such as quantum computing, artificial intelligence (AI)[31], and virtual and augmented reality (VR and AR), and how the Security Rule would apply in each case. The full list of new technologies and how the Security Rule applies to each of the new technologies is provided in the Proposed Rule (pg. 289-298).

OCR requests comments on how the Security Rule protects ePHI used in new and developing technologies, including any benefits, drawbacks, or unintended consequences. **OCR also requests comments on the following additional considerations:**

- **Whether OCR's understanding of how the Security Rule applies to new technologies involving ePHI is not comprehensive and if so, what issues should also be considered.**
- **Whether there are technologies that currently or in the future may harm the security and privacy of ePHI in ways that the Security Rule could not mitigate without modification, and if so, what modifications would be required.**
- **Whether there are additional policies or technical tools that the Department may use to address the security of ePHI in new technologies**

What's Next?

Vizient's Office of Public Policy and Government Relations looks forward to hearing continued member feedback on this Proposed Rule. This feedback will help inform our comments to the agency. Stakeholder input plays a major role in shaping future changes to policy. We encourage you to reach out to our office if you have any questions or regarding any aspects of this proposed regulation – both positive reactions and provisions that cause you concern. Please direct your feedback to Jenna Stern, AVP Regulatory Affairs and Public Policy in Vizient's Washington, D.C. office.

[31] 2024-30983.pdf