HIPAA Security Proposed Rule – Summary
January 15, 2025

On December 27, 2024, the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) issued a Notice of Proposed Rulemaking (NPRM) to modify the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. This proposal is intended to strengthen cybersecurity protections for electronic protected health information (ePHI). OCR administers and enforces the Security Rule, which establishes national standards for the protection of individuals' ePHI by covered entities (health plans, healthcare clearinghouses, and most healthcare providers), and their business associates (together, "regulated entities"). You can find the proposed rule here, and the HHS press release and fact sheet here, and here. Comments are due March 7, 2025. Also, for reference purposes, the current regulatory text (as contrasted with what is proposed in the rule outlined below), can be found here.

I. Key Takeaways

- OCR says regulated entities are failing to perform compliant risk analyses and policy changes are needed and that only 14 percent of covered entities and 17 percent of business associates are currently in compliance.
- Maintaining an asset inventory is not explicitly required under the current Security Rule but OCR calls it a "fundamental component of conducting a risk analysis" and says many healthcare organizations (HCOs) are not maintaining these inventories. In place of the existing standard for security management process OCR proposes to 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 (CIA) of ePHI. OCR calls for this to happen no less than every 12 months or following a significant event.
- OCR has proposed a compliance date of 180 days after the effective date of the final rule, which is 240 days after its publication.
- OCR is proposing to remove "addressable" implementation standards and make all standards required. OCR would allow regulated entities to determine the security measures that are reasonable and appropriate to fulfill the required standards and implementation specification and that there would be a variety of ways to achieve compliance.
- While OCR recognizes challenges small and rural healthcare providers face, they feel it's just as important for small and rural healthcare providers to implement strong security measures as it is for larger ones.
- **NOTE:** There is a likelihood that the incoming Trump administration will freeze this rule along with several others. Until or unless that happens, CHIME plans to submit comments. More will be known in the days following the start of the new administration. Please review our Monday e-newsletter – the Washington Debrief – for breaking news. To subscribe, please reach out to us at policy@chimecentral.org and we will add you.

II. Background

HIPAA was signed into law 1996 and the Security Rule was initially finalized and published in 2003. HIPAA was amended in 2009 by the Health Information Technology for Economic and Clinical Health (HITECH) Act to mandate stronger safeguards for protecting ePHI in 2009. Congress amended HITECH with H.R. 7898 which resulted in P.L. 116-321 in 2021. It requires HHS to take into account a regulated entities' use of recognized security practices when enforcing the Security Rule. This change in law was a direct result of CHIME advocacy.

The Biden administration has issued a proposal which re-opens and would update the rule to "increase cybersecurity for ePHI" by addressing:

- Changes in the environment in which healthcare is provided;
- Significant increases in breaches and cyberattacks;
- Common deficiencies OCR has observed in investigations into Security Rule compliance by regulated entities;
- Other cybersecurity guidelines, best practices, methodologies, procedures, and processes; and
- Court decisions that affect enforcement of the Security Rule.

While OCR does not believe that their proposed changes will prevent all breaches, they do believe that it will prevent many and enable regulated entities to respond more quickly when there is a "significant event," including a cyber incident. OCR states: "Today, cybersecurity is a concern that touches nearly every facet of modern healthcare, certainly more than it did in 2003 or even 2013." They note the growing escalation in cyberattacks and breaches impacting 500 or more individuals and the negative impact these incidents can have on patient care. OCR further notes that there is a growing patchwork of state-specific laws aimed at protecting PHI, which may create difficulties for regulated entities that are located or operate in multiple states, and none address protecting ePHI specifically.

President Biden designated the Healthcare and Public Health (HPH) Sector as a critical infrastructure sector and HHS as the Sector Risk Management Agency (SRMA) and directed federal agencies to establish and implement minimum requirements for risk management.

III. Overview of Proposed Policies

OCR's justification for re-opening the Security Rule includes the following reasons:

- Significant transformation undergone by the healthcare sector in last decade;
- High value that stolen medical records fetch by cyber criminals;
- Increased risk to ePHI posed by artificial intelligence (AI);
- Other threats to ePHI like internal actors and system outages like Crowdstrike;
- Inconsistent use of cyber best practices;
- Failures by HCOs to maintain "a current inventory of sensitive and valuable data and where those reside";
- Need for regulatory clarity given the recent court case, *University of Texas M.D. Anderson Cancer Center v. HHS* ("M.D. Anderson"), where the U.S. Court of Appeals for the Fifth Circuit vacated a $4.3 million fine finding security mechanisms need not be effective or implemented throughout an enterprise. The court found that, "the Security Rule does not say anything about how effective a mechanism for encryption must be," and thus "under the court's interpretation, a regulated entity can meet its obligations under the Security Rule concerning encryption and decryption of ePHI by implementing a mechanism to do so, without regard for the effectiveness of the implementation."

The court also said that asking employees to sign an agreement that requires encryption of portable devices as sufficient to meet the Security Rule and HHS disagreed with this interpretation; and

- HHS' HIPAA advisory body, the National Committee on Vital and Health Statistics (NCVHS), made several recommendations to OCR on how they could improve the Security Rule including removing addressable implementation specifications because many are treating this as a choice as opposed to adopting a reasonable alternative.

OCR is proposing that regulated entities would have until the "compliance date" (i.e., 240 days after publication) to establish and implement policies, procedures, and practices to achieve compliance with any new or modified standards. In other words, regulated entities must comply with the applicable new or modified standards or implementation specifications no later than this date.

OCR does not propose to adopt referenced best practices as the standard or implementation specifications unless otherwise specified in the proposed regulatory text but there are discussions and references to certain **HHS Cybersecurity Performance Goals (CPGs)** and National Institute of Standards and Technology (NIST) guidance, among others, throughout the proposed rule.

Please see our crosswalk to the rule and HHS' CPGs here.

IV. Definitions

A. Section 160.103 (page 72)

OCR proposes to update the definition of "electronic media" to include media used for recording, maintaining, or processing data, while at rest, in transit, or in process. This change emphasizes the need to protect data in process, as it is vulnerable to breaches when unencrypted.

Additionally, to ensure that the definition includes future technology, OCR proposes to add to the list of examples "any other form of digital memory or storage" on which data may be recorded, maintained, or processed.

OCR further proposes to revise the definition of "transmission media" to reflect that data is mostly transmitted electronically today, with a limited exception for handwritten data. Public networks will be included as examples of transmission media. A technical correction will replace "electronic storage media" with "electronic storage material" to ensure consistency in definitions.

B. Section 164.304—Definitions (page 76)

OCR proposes to add ten new terms and modify the definitions of fifteen existing terms.The proposed new regulatory terms would be: Deploy, Implement, Electronic information system, Multi-factor Authentication, Relevant Electronic Information System, Risk, Technical controls, Technology Asset, Threat, and Vulnerability.

OCR proposes to modify the following terms: Access, Administrative safeguards, Authentication, Availability, Confidentiality, Information System, Malicious Software, Password, Physical Safeguards, Security or Security Measures, Security Incident, Technical Safeguards, User, and Workstation.

1. Clarifying the Definition of "Access" (pages 76 and 356)

OCR is proposing to expand the list of activities that should be considered under the term by adding the activities of "deleting" and "transmitting." They also propose to replace "system resource" with

"component of an information system" which would clarify that the term includes any and all components of an information system and an information system as a whole.

2. **Clarifying the Definition of "Administrative Safeguards" (pages 77 and 356)**

To address the minor inconsistencies between the definitions of "administrative" and "physical" safeguards and to ensure that each is afforded an equal weight of importance, OCR proposes the following changes:

> *Administrative safeguards are administrative actions and related policies and procedures to manage the selection, development, implementation, and maintenance (including updating and modifying) of security measures to protect ePHI, and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.*

3. **Clarifying the Definition of "Authentication" (pages 78 and 356)**

OCR proposes to clarify the definition of "authentication" to mean corroboration that either a person or technology asset is the one they are claiming to be.

4. **Clarifying the Definition of "Availability" (pages 79 and 356)**

Given the increased connectivity of the healthcare environment, OCR proposes to clarify the definition of "availability" to mean the property that data or information is accessible and usable upon demand by an authorized person or technology asset.

5. **Clarifying the Definition of "Confidentiality" (pages 80 and 356)**

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

6. **Adding Definitions of "Deploy" and "Implement" (pages 80 and 356)**

OCR is concerned that some regulated entities are interpreting the requirement to implement technical policies and procedures to mean they are only required to establish written policies and procedures but do not need to apply effective, automated technical policies and procedures to all ePHI throughout their enterprise. OCR references the *M.D. Anderson v. HHS* case as justification for these proposals. OCR proposes to define the term "deploy" to mean to configure technology for use and implement such technology.

OCR proposes to define the term "implement" to clarify that a safeguard must be put into place and be in effect throughout the enterprise, as opposed to only some components of a regulated entity's relevant information systems (e.g., some laptops or servers) or applied to a subset of ePHI. OCR proposes to expressly clarify that implement also means that a safeguard must function as expected.

Under this proposal, OCR would not consider a safeguard to be implemented if it is not functioning in the manner in which it is expected. They further state that, "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." Proposed definition below.

Implement means to put into effect and be in use, operational, and function as expected throughout the covered entity or business associate.

7. Adding a Definition of "Electronic Information System" (pages 83 and 356)

OCR proposes to add a definition of "electronic information system" to better distinguish the concept from the broader category of an information system and calls for limiting the definition to an interconnected set of electronic information resources under the same direct management control that shares common functionality. The proposed definition is:

Electronic information system means interconnected set of electronic information resources under the same direct management control that shares common functionality. An electronic information system generally includes technology assets, such as hardware, software, electronic media, information, and data.

8. Modifying the Definition of "Information System" (pages 84 and 357)

OCR proposes to modify the definition of "information system," to clarify that an information system "generally, not just "normally," includes hardware, software, data, communications, and people. OCR gives the following example: "both a healthcare provider and a cloud-based EHR vendor have direct management control over the ePHI in the cloud-based EHR. Accordingly, such ePHI generally is part of both the information system of the healthcare provider and of the cloud-based EHR vendor." They also clarify that, "a technology asset may be included as part of the information systems of multiple regulated entities where such regulated entities all have direct management control over the technology asset." 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. Modifying the Definition of "Malicious software" (pages 85 and 357)

OCR proposes to replace the current definition of malicious software to define it to mean software or firmware intended to perform an unauthorized action or activity that will have adverse impact on an electronic information system and/or the confidentiality, integrity, or availability (CIA) of ePHI. Thus, it would clarify that malicious software could include either software or firmware and that the negative effects of the malicious software may not be limited to damaging or disrupting a system. Rather, effects of the software could be intended to have any type of adverse impact on an electronic information system and/or the CIA of ePHI. OCR further proposes to include in regulatory text a non-exhaustive list of examples, such as viruses, worms, Trojan horses, spyware, and some forms of adware, to assist regulated entities in understanding what constitutes malicious software.

10. Adding a Definition of "Multi-factor Authentication" (MFA) (pages 86 and 357)

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

- Information known by the user, including but not limited to a password or personal identification number (PIN).

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

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

OCR points to HHS' 405(d) Program's "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients" (HICP) as rationale for inclusion.

11. Clarifying the Definition of "Password" (pages 89 and 357)

OCR proposes to add examples to the definition of "password" to further clarify what constitutes a character, and adds "such as letters, numbers, spaces, other symbols" to the existing definition. They believe these regulatory examples would provide necessary context for regulated entities that deploy safeguards involving passwords.

12. Clarifying the Definition of "Physical Safeguards" (pages 89 and 357)

OCR proposes to clarify that the policies and procedures referred to in the definition are those that specifically are related to physical measures, and to replace "buildings" with "facilities" because facility is a defined term under the Security Rule and has an equivalent meaning. OCR says they always intended that physical safeguards apply to any location where a regulated entity might possess ePHI, including the physical premises and interior and exterior of a building, and any location that might affect the CIA of ePHI. Additionally, given the mobility of technology today, including workstations that may access ePHI, OCR believes it would be more appropriate to use the term facility to make clear that the physical safeguards are to apply throughout the premises of the regulated entity. Thus, their new definition is:

> *Physical safeguards are physical measures and related policies and procedures to protect a covered entity's or business associate's relevant electronic information systems, and related facilities and equipment, from natural and environmental hazards and unauthorized intrusion.*

13. Adding a Definition of "Relevant Electronic Information System" (pages 90 and 357)

OCR proposes to add the term "relevant electronic information system" to mean an electronic information system that creates, receives, maintains, or transmits ePHI or that otherwise affects the CIA of ePHI. This proposal is intended to further clarify the scope of regulated entities' compliance obligations, including the obligation of regulated entities to understand the relationship between their various electronic information systems and the CIA of ePHI. One example they offer is a covered entity's food and beverage or gift shop systems.

Cybercriminals may be able to access ePHI by leveraging vulnerabilities in electronic information systems that do not themselves create, receive, maintain, or transmit ePHI where they are connected to or can affect those that do. Thus, OCR interprets an electronic information system as otherwise affecting the CIA of ePHI if it is insufficiently segregated physically and electronically from an electronic

information system that creates, receives, maintains, or transmits ePHI or one that otherwise affects the CIA of ePHI.

An electronic information system would also fit the category of “otherwise affecting” if it contains information that relates to an electronic information system that creates, receives, maintains, or transmits ePHI or to another electronic information system that otherwise affects the CIA of ePHI. OCR provides several examples of this, including an electronic information system that contains the decryption keys for a regulated entity's encryption algorithms.

14. Adding a Definition of “Risk” (pages 92 and 358)

OCR believes that defining the term “risk” would clarify several existing and proposed provisions of the Security Rule – including the factors regulated entities must consider when determining the security measures they will implement and the importance and purpose of conducting the required risk analysis. OCR proposes to define this term as:

> *Risk means the extent to which the confidentiality, integrity, or availability of ePHI is threatened by a potential circumstance or event.*

15. Clarifying the Definitions of “Security or Security Measures” and “Security Incident” (pages 93 and 358)

OCR proposes to modify the definition of “security or security measures.” OCR says, “The existing definition does not make clear that a security incident may result from two types of behaviors—those related to attempted or successful but unauthorized access, use, disclosure, modification, or destruction of information in an information system, and those that are related to the attempted or successful unauthorized interference with system operations in an information system.” Proposed definition below:

> *Security or security measures encompass all of the administrative, physical, and technical safeguards in or applied to an information system. Security incident means any of the following: (1) The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information in an information system. (2) The attempted or successful unauthorized interference with system operations in an information system.*

16. Adding Definitions of “Technical Controls” (pages 95 and 358)

OCR proposes to add and define the term “technical controls” to mean:

> *Technical controls means the technical mechanisms contained in the hardware, software, or firmware components of an electronic information system that are primarily implemented and executed by the electronic information system to protect the information system and data therein.*

17. Modifying the Definition of “Technical Safeguards” (pages 96 and 358)

OCR proposes to modify the definition of “technical safeguards” to mean:

> *The technology, technical controls, and related policies and procedures governing the use of the technology that protects and controls access to electronic protected health information.*

18. Adding a Definition of "Technology Asset" (pages 96 and 358)

OCR proposes to distinguish the requirements that apply to all components of an electronic information system vs. those that only apply to certain components. Proposed definition below:

> *Technology asset means the components of an electronic information system, including but not limited to hardware, software, electronic media, information, and data.*

19. Adding a Definition of "Threat" (pages 97 and 358)

OCR plans to define the term "threat" broadly and to include hackers, malicious insiders, and malicious software. Proposed definition below:

> *Threat means any circumstance or event with the potential to adversely affect the confidentiality, integrity, or availability of electronic protected health information.*

20. Clarifying the Definition of "User" (pages 98 and 358)

OCR proposes to clarify the definition of user as a person with authorized access.

21. Adding a Definition of "Vulnerability" (pages 98 and 358)

OCR plans to define "vulnerability" largely as NIST has to mean:

> *A flaw or weakness in an information system, information system security procedures, design, implementation, or technical controls that could be intentionally exploited or accidentally triggered by a threat.*

22. Clarifying the Definition of "Workstation" (pages 100 and 358)

OCR proposes to modernize the definition of "workstation" to mean:

> *An electronic computing device and electronic media stored in its immediate environment. Workstation includes but is not limited to the following types of devices: a server, desktop computer, laptop computer, virtual device, and mobile device such as a smart phone or tablet.*

V. Security Standards: General Rules - Section 164.306 (page 102)

OCR is concerned that regulated entities are misinterpreting the general requirements of the Security Rule such that it applies to only some ePHI, rather than all ePHI. They are furthermore concerned that many are misconstruing the difference between required and addressable implementation specifications and are treating addressable ones as optional. They state, "we must squarely confront the problem of regulated entities treating addressable implementation specifications as optional. Relatedly, we also believe that we must consider modifying the Security Rule to set an acceptable minimum level of security specifications."

OCR proposes to remove the distinction between "required" and "addressable" standards stating: "Importantly, removing the distinction between required and addressable would not eliminate all of the Security Rule's flexibility and scalability. Instead, it would simply clarify for regulated entities where the floor of protection must lie, and regulated entities must implement solutions that meet that floor, taking into consideration their needs and capabilities." They offer the following illustrative examples:

> *For example, a small or rural healthcare provider must implement a solution that ensures the protection of ePHI in the manner required by the Security Rule, but the specific solution that it*

chooses would reflect consideration of its particular circumstances, including available resources. In some cases, a small or rural healthcare provider might opt to implement a cloud-based EHR or other software solution that could reduce the healthcare provider's need to separately invest in data storage, backup systems, and IT personnel. And in other circumstances, a small or rural healthcare provider might choose to contract with a third party to provide IT support, rather than hiring its own workforce members to perform such functions.

The agency also proposes to require each regulated entity to protect against any reasonably anticipated threats or hazards to the CIA of all ePHI, instead of to the security or integrity of ePHI. Additionally, OCR calls for requiring each regulated entity to ensure that its workforce complies not only with the Security Rule, but also all administrative, physical, and technical safeguards. OCR clarifies that regulated entities are to apply reasonable and appropriate security measures to implement the standards and implementation specifications of the Security Rule.

OCR proposes to add a new element to the list of factors that regulated entities must take into account when deciding whether a particular security measure is reasonable and appropriate for implementing a standard: the effectiveness of the security measure in supporting the resiliency of the regulated entity. Said another way, OCR states they propose "to require a regulated entity to consider the ability of its implementation of a particular security measure to aid it in preventing, withstanding, and recovering from an emergency or other occurrence that affects the CIA of ePHI, including a successful security incident."

OCR also proposes to remove the maintenance implementation specifications for specific standards, when applicable.

VI. Administrative Safeguards - Section 164.308 (page 113)

OCR says that "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." They reiterate their concerns around the treatment of addressable standards.

OCR is not proposing covered entities implement any new safeguards to ensure their business associates are in compliance. However, because OCR has learned that business associates are not employing appropriate safeguards and that some "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," OCR is calling for where a regulated entity is required to meet a certain security measure that they be required to review and test it on a specified cadence, and to modify the measure as reasonable and appropriate. This includes, "verifying that the security measures work as designed and that workforce members know how to implement them." They offer the following 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.

OCR proposes to require that a regulated entity implement and document, in writing, its implementation of the proposed administrative safeguards required by the Security Rule.

A. Standard: Technology asset inventory - Section 164.308(a)(1)(i) (pages 121 and 360)

In place of the existing standard for security management process OCR proposes to 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 CIA of ePHI. OCR states, "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," and goes onto add that, "Regulated entities cannot understand the risks to the confidentiality, integrity, and availability of their ePHI without a complete understanding of these assets."

OCR states regulated entities should determine the movement of ePHI through, into, and out of their information systems and to describe such movement in a network map. OCR states that, "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." OCR further proposes to require regulated entities as part of the asset inventory to:

a. Determine the movement of ePHI through, into, and out of its information systems and to describe such movement in a network map.
b. Establish a written inventory that contains their technology assets to include those that create, receive, maintain, or transmit ePHI and those that do not but that may affect the CIA of ePHI.
c. Include the identification, version, person accountable for, and location of each of the assets or information system components.
d. Review and update the written inventory of technology assets and the network map in the following circumstances:
    a. On an ongoing basis, but <u>at least once every 12 months</u>; and
    b. When there is a change in the regulated entity's environment or operations that may affect ePHI. This includes, but is not limited to, upgrading, updating, or patching of technology assets, sales, transfers, mergers, security incidents, and changes to federal, state or local laws.
e. 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.
    a. *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 healthcare 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 healthcare provider's network map.*

OCR says their proposal aligns with **HHS' enhanced CPG for Asset Inventory** which requires that a regulated entity identify assets to more rapidly detect and respond to potential risks and vulnerabilities.

B. Standard: Risk Analysis - Section 164.308(a)(2)(i) (pages 127 and 361)

OCR states that there are numerous methods of performing a risk analysis and points to existing guidance that can help, including HHS' Security Risk Assessment Tool, as well as NIST guidance. OCR "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." OCR offer numerous examples of how they anticipate regulated entities can handle different risk levels on page 132.

OCR restates their concerns that regulated entities are not performing compliant risk analyses and reiterates that: "The responsibility to maintain an appropriate risk analysis rests with the regulated entity (emphasis added)." As noted earlier, OCR is proposing to elevate the requirement to conduct a risk analysis. OCR proposes eight implementation specifications for the risk analysis standard, consistent with previously issued guidance. The proposed implementation specification for a written assessment would require the regulated entity, at a minimum, to perform and document all of the following:

1. Review the technology asset inventory and the network map to identify where ePHI may be created, received, maintained, or transmitted within its information systems.
2. Identify all reasonably anticipated threats to the confidentiality, integrity, and availability of ePHI that it creates, receives, maintains, or transmits.
3. 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 CIA of ePHI.
4. 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.
5. Make a reasonable determination of the likelihood that each identified threat would exploit the identified vulnerabilities.
    a. 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.
6. Make a reasonable determination of the potential impact of each identified threat should it successfully exploit the identified vulnerabilities.
    a. 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.
7. Create an assessment of risk level for each identified threat and vulnerability.
8. Create an assessment of risks to ePHI posed by entering into or continuing a business associate agreement (BAA) or other written arrangement with any prospective or current business associate, based on the written verification obtained from the prospective or current business associate.

The risk analysis should be reviewed, verified, and updated on an ongoing basis, no less 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.

C. Standard: Evaluation - Section 164.308(a)(3)(i) (pages 137 and 362)

OCR proposes to revise the Evaluation Standard, such that a regulated entity consider 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. They also call for deleting the requirement that the evaluation be performed "based initially on the standards implemented under this rule" and adding two implementation specifications:

- Conducting an evaluation within a reasonable period of time before making a change to its environment or operations.
- Requiring a regulated entity to respond to the evaluation in accordance with its risk management plan.

D. Standard: Patch Management - Section 164.308(a)(4)(i) (pages 140 and 363)

The proposed rule contains a lengthy discussion of the virtues of patching and cites the growing incidence of cyberattacks. Thus, 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 so that regulated entities are aware of their liability for appropriately safeguarding ePHI. They have proposed six implementation specifications that 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 CIA of ePHI. A regulated entity would be required to:

- Review their patch management written policies and procedures at least once every 12 months and modify as reasonable and appropriate.
- Patch, update, and upgrade the configurations of relevant electronic information systems in accordance with its written policies and procedures and based on the results of a regulated entity's: risk analysis; vulnerability scans; monitoring of authoritative sources; and penetration tests.
    - This must be done within "a reasonable and appropriate period of time," defined by OCR as "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."
    - Within 30 calendar days of identifying the need to address a high risk, a regulated entity must patch, update, or upgrade the configuration of a relevant electronic information system where a patch, update, or upgrade is available; or, where a patch, update, or upgrade is not available, within 30 calendar days of a patch, update, or upgrade becoming available.
    - For all other patches, updates, or upgrades to the configurations of relevant electronic information systems, a reasonable and appropriate period of time would be determined by the regulated entity's written policies and procedures.
    - **Exceptions:**

- A regulated entity would be required to document that an exception applies and that all other applicable conditions are met.
- Exception #1: When no patch / update / upgrade is available to address a risk identified in the regulated entity's risk analysis.
- Exception #2: When the only available patch / update would adversely affect the CIA of ePHI.
- A regulated entity would be required document in real-time the existence of the applicable exception and to implement reasonable and appropriate compensating controls.
- 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 until such time as a patch / update / upgrade that does not adversely affect ePHI becomes available.

OCR says their proposal aligns with **HHS' enhanced CPG for Cybersecurity Mitigation** by requiring a regulated entity to prioritize and mitigate vulnerabilities discovered by vulnerability scanning and penetration testing.

E. Standard: Risk Management - Section 164.308(a)(5)(i) (pages 145 and 365)

OCR proposes to elevate the implementation specification for risk management to a standard to require a regulated entity to establish and implement a plan for reducing the risks identified through its risk analysis activities. Specifically, a regulated entity must implement security measures "sufficient to reduce risks and vulnerabilities to all ePHI to a reasonable and appropriate level." OCR notes that what is "reasonable and appropriate" is circumstance-dependent OCR proposes four required implementation specifications:

A. **Planning** - Establish and implement a written risk management plan for reducing risks to all ePHI "to a reasonable and appropriate level." "Reasonable and appropriate" is circumstance-specific and depends on the criticality of the risks identified and can take into account size, needs and capabilities, risk profile, ability of security measures to reduce or eliminate a particular identified risk or vulnerability, and the ubiquity of such security measures.
B. **Maintenance** - This must occur at least once every 12 months.
C. **Prioritize** - Establish a written risk management plan to prioritize the risks identified in the regulated entity's risk analysis based on the risk levels.
D. **Implementation** - Implement security measures in a timely manner to address the risks identified.

OCR says their proposal aligns with **HHS' essential CPG to Mitigate Known Vulnerabilities**.

F. Standard: Sanction Policy - Section 164.308(a)(6)(i) (pages 147 and 365)

OCR proposes to elevate the implementation specification for sanction policy to a standard addressing workforce members.as this is a tool for applying appropriate sanctions to workforce members who fail to comply with security requirements. OCR states: "Thirty-one percent of respondents indicated that the data loss or exfiltration was caused by a failure of workforce members to follow organizational policies." OCR has not proposed changing the language of the existing standard, but they have proposed three implementation specifications:

1. Establish written policies and procedures for sanctioning workforce members who fail to comply with the regulated entity's security policies and procedures.
2. Review written sanctions policies and procedures at least once every 12 months and modify as appropriate.
3. Apply appropriate sanctions against workforce members who fail to comply and document when it sanctions a workforce member and why.

A regulated entity may structure its sanction policies in the manner most suitable to their organization and offers details on page 150 on sanction policies.

G. Standard: Information System Activity Review - Section 164.308(a)(7)(i) (pages 151 and 366)

OCR proposes to elevate the existing implementation specification for information system activity review to a standard to better help a regulated entity detect and prevent data leakage initiated by malicious authorized users. OCR proposes five implementation specifications:

1. **Written policies** - Establish written policies and procedures for retaining and reviewing records of activity.
2. **Record review** - Records of activity would include audit trails, event logs, firewall logs, system logs, data backup logs, access reports, anti-malware logs, and security incident tracking reports.
3. **Record Retention** - For a period of time that is reasonable and appropriate for the type of report or log.
4. **Response** - Respond in accordance with the covered entity's or business associate's security incident response plan for suspected or known security incident.
5. **Maintenance** - Review and test the written policies and procedures at least once every 12 months.

H. Standard: Assigned Security Responsibility - Section 164.308(a)(8) (pages 156 and 367)

The purpose of this standard is to identify who would be operationally responsible for assuring that the regulated entity complies with the Security Rule, which OCR proposes to modify as:

> *In writing, identify the security official who is responsible for the development and implementation of the policies and procedures, written or otherwise, and deployment of technical controls required by this subpart for the covered entity or business associate.*

I. Standard: Workforce Security - Section 164.308(a)(9)(i) (pages 157 and 367)

OCR proposes that a regulated entity must:

1. **Authorization and / or supervision** - Establish and implement written procedures for the authorization and/or supervision of workforce members who have access to ePHI or who work in facilities where ePHI or relevant information systems might be accessed.
2. **Workforce clearance procedure** - Establish and implement written procedures to determine that the access of a workforce member to ePHI / relevant electronic information systems is appropriate.
3. **Modification of termination procedures** - Establish and implement written procedures to terminate a workforce member's access to ePHI and relevant electronic information systems. It

would require that their access be terminated as soon as possible, but not later than one hour after the workforce member's employment or other arrangement ends.
4. **Notification** - Establish and implement written procedures to notify another covered entity or business associate of a change in or termination of access. Notification must occur as soon as possible but no later than 24 hours after a change in or termination of a workforce member's authorization to access.
5. **Maintenance** - Review and test written workforce security policies and procedures at least once every 12 months, and modify as reasonable and appropriate.

OCR says their proposal aligns with **HHS' 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.

J. Standard: Information Access Management - Section 164.308(a)(10)(i) (pages 164 and 368)

OCR is proposing to require regulated entities establish and implement written policies and procedures for authorizing access to ePHI and relevant electronic information. The agency proposes to modify three of the associated existing implementation specifications and to add three new implementation specifications:

a. **Isolating healthcare clearinghouse functions** - If a healthcare clearinghouse is part of a larger organization, the clearinghouse must 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.
b. **Access authorization** - Establish and implement written policies and procedures for granting and revising access to ePHI and relevant electronic information systems as necessary and appropriate for each prospective user and technology asset to carry out their assigned function(s).
c. **Authentication management (NEW)** - Establish and implement written policies and procedures for verifying the identities of users and technology assets prior to accessing the covered entity's or business associate's relevant electronic information systems, including written policies and procedures for implementing MFA technical controls.
d. **Access determination and modification** - Establish and implement written policies and procedures that determine, document, review, and modify the access of each user and technology asset to specific components of the covered entity's or business associate's relevant electronic information systems.
e. **Network segmentation (NEW)** - Establish and implement written policies and procedures that ensure that a covered entity's or business associate's relevant electronic information systems are segmented to limit access to ePHI to authorized workstations.
f. **Maintenance (NEW)** - Review and test the written policies at least once every 12 months, and modify as reasonable and appropriate.

K. Standard: Security Awareness Training - Section 164.308(a)(11)(i) (pages 170 and 369)

OCR proposes to rename and redesignate the standard for security awareness and training. Under their proposal, a regulated entity would be required 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)." OCR proposes four implementation specifications requiring regulated entities 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.
- Guarding against, detecting, and reporting suspected or known security incidents, including but not limited to malicious software and social engineering.
- 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. OCR does not propose that passwords be required to meet a particular standard.

OCR also calls for replacing the implementation specification for periodic security updates with one addressing the timing and frequency of security awareness training and calls for requiring regulated entities provide this training to each member of their workforce by the compliance date for this rulemaking, if finalized, and at least once every 12 months thereafter. OCR further states that this requires regulated entities 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. As an example they offer, "if the entity implements a new EHR system, it would be required to also train its workforce, as appropriate, on measures to guard against security incidents related to the installation, maintenance and/or use of the system."

OCR also proposes to require regulated entities to provide workforce members with ongoing education, which includes reminders about new and emerging threats. Finally, OCR proposes to require a regulated entity to document that it has provided training and ongoing reminders to its workforce members.

OCR says their proposals align with **HHS' essential CPG for Basic Cybersecurity Training** because it requires educating users on how to access ePHI and 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.

L. Standard: Security Incident Procedures Section 164.308(a)(12)(i-ii) (pages 174 and 371)

OCR proposes redesignating the standard for security incident procedures and clarifying their expectations by adding a requirement to establish a 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. OCR does not dictate the form, format, or content of such report. A regulated entity would be required to implement written procedures for testing and revising the security incident response plan(s) and review and test its security incident response plans at least once every 12 months and document the results of such tests.

OCR also calls for redesignating the implementation specification for response and reporting and renaming it "Response," and making two modifications to the existing language related to identifying and responding to suspected or known security incidents and for mitigating, to the extent practicable, the harmful effects of suspected or known security incidents. They also propose adding new language to the standard that would require a regulated entity to identify and remediate the root cause(s) of

suspected or known security incidents to the extent practicable and eradicate the security incidents that are suspected or known to the regulated entity. OCR says they, “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.”

Regulated entities would be required to “develop and maintain documentation of investigations, analyses, mitigation, and remediation for security incidents that are suspected or known.” This includes verbal reports of a suspected or known security incident. Documentation of such would need to be maintained for six years.

OCR states that their proposal aligns 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, **the essential CPG for Basic Incident Planning and Preparedness** to have effective responses to and recovery from security incidents. **and the enhanced CPG for Centralized Incident Planning and Preparedness** by requiring a regulated entity to maintain, revise, and test security incident response plan.

M. Standard: Contingency Plan - Section 164.308(a)(13)(i) (pages 178 and 371)

OCR proposes to 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. Regulated entities would be required 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. OCR says this is not limited to electronic information systems that create / receive / maintain / transmit ePHI because other electronic information systems and/or technology assets “may be crucial to ensuring the CIA of ePHI, providing patient care, and supporting other business needs.”

OCR also proposes to clarify the procedures to create and maintain exact retrievable copies of ePHI must be in writing and have written procedures to restore both its critical relevant electronic information systems and data within 72 hours of the loss. OCR further proposes regulated entities review and implement their procedures for testing contingency plans at least once every 12 months, and document the results and modify their plans as needed.

N. Standard: Compliance Audit - Section 164.308(a)(14) (pages 181 and 373)

OCR proposes a new standard for compliance audits, requiring 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. The current requirement is that regulated entities conduct internal or third-party compliance audits. OCR is not planning on dictating whether the compliance audit should be performed by the regulated entity or an external party.

O. Standard: Business Associate Contracts and Other Arrangements - Section 164.308(b)(1-2) (pages 182 and 393)

The Security Rule’s current requirements hold that regulated entities obtain written satisfactory assurances that their business associate(s) will appropriately safeguard ePHI, but does not require a regulated entity to verify that entities that create / receive / maintain / transmit ePHI on their behalf are in indeed taking needed steps to protect ePHI. OCR feels this leaves “a gap in protections from risks to

ePHI related to regulated entities' vendors and supply chains." Thus, OCR is proposing several changes including regulated entities securing greater assurance from business associates and their subcontractors are doing what is needed to safeguard ePHI. This includes:

1. Regulated entities verifying that a business associate has deployed the required technical safeguards at least once every 12 months and obtaining satisfactory assurances that its business associate would comply with the Security Rule.
2. Verification would need to include a written analysis of the business associate's relevant electronic information systems and need to be performed by a person with appropriate knowledge of and experience with generally accepted cybersecurity principles and who has the authority to act on behalf of the business associate 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 says this aligns with the **Essential CPG for Vendor/Supplier Cybersecurity Requirements** which calls for regulated entities to identify, assess, and mitigate risks to ePHI used by or disclosed to business associates.

P. Standard: Delegation To Business Associate - Section 164.308(b)(3) (pages 185 and 374)

OCR proposes a new standard for delegation to a business associate because they believe "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." OCR clarifies that a regulated entity may permit a business associate to serve as its designated security official but reminds that regulated entities remain liable for compliance with the Rule.

VII. Physical Safeguards - Section 164.310 (pages 189 and 374)

OCR proposes to clarify that physical safeguards be applied to all ePHI throughout the regulated entity's facilities, remove any distinction between addressable and required implementation specifications, and modify all four physical safeguard standards to require that the requisite policies and procedures be in writing and implemented throughout the enterprise. OCR calls for requiring a regulated entity to maintain its security measures by reviewing and testing the required security measures at least once every 12 months, and by modifying the same as reasonable and appropriate. They furthermore call for modifying the four related physical security standards as follows.

1. **Facility Access Controls - Section 164.310(a)(1) (page 197):**
    a. Must be in writing and address physical access to all relevant systems.
    b. Modify the implementation specifications for contingency operations, facility security plan, and access control and validation procedures requiring established and implemented policies and procedures and that they be in writing.
    c. Require written procedures to both authorize and manage a person's role-based access to facilities.
    d. Require written procedures on security cameras.
2. **Workstation Use - Section 164.310(b)(1) and**
3. **Workstation Security - Section 164.310(c) (page 198):**
    a. Must be in writing and address physical access to all relevant systems.

b. Specify the physical attributes of workstation surroundings, including the removal of workstations from a facility and the movement of workstations within and outside of a facility.
c. Require physical safeguards for workstations that access ePHI or relevant electronic information systems to comply with its written policies and procedures for workstation use.
d. Encourages – but does not require - whether there are workstations located in public areas or other areas that are more vulnerable to theft, unauthorized use, or unauthorized viewing; whether such devices should be relocated and whether more security measures are needed.
e. Provide role-based security awareness and training on physical safeguards that it has implemented, particularly those policies and procedures for mobile devices.

4. **Technology Asset Controls - Section 164.310(d)(1) (page 200):**
    a. Renamed from “Device and media controls.”
    b. Replacing “hardware and electronic media” with “technology assets.”
    c. Workstation includes mobile devices.
    d. Procedures must be in place and maintained.
        i. Written policies for disposal of ePHI and sanitization of electronic media be tied to current standards for sanitizing electronic media before the media are made available for re-use.

VIII. Technical Safeguards - Section 164.312 (pages 204 and 376)

OCR clarifies and proposes to require that regulated entities both document and implement their technical safeguards. They propose to add maintenance requirements separately to the implementation specifications for particular technical safeguards. OCR also proposes to remove the distinction between required and addressable implementation specifications and make all implementation specifications required, with limited exceptions.

A. Access Control - Section 164.312(a)(2)(i-viii) (pages 213 and 376)

OCR proposes to clarify the standard for access control by requiring a regulated entity to deploy technical controls in relevant electronic information systems to allow access only to those users and technology assets that have been granted access rights. They are not proposing a specific type of access control method or technology to deploy. They call for removing the distinction between required and addressable implementation specifications. Finally, they are elevating encryption and decryption to a standard. OCR also proposes to add five new implementation specifications, redesignate the implementation specification for encryption and decryption as a standard, and modify and rename the unique user identification specification as follows:

1. **Unique user identification** – Standard renamed and modified calling for:

    Assigning a unique name, number, and/or other identifier for tracking each user and technology asset in the covered entity or business associate’s relevant electronic information systems.

    OCR says this aligns with the **HHS’ essential CPG for Unique Credentials**, which calls for regulated entities to use unique credentials to help detect and track anomalous activities.

2. **Administrative and increased access privileges [NEW] –** OCR proposes:

   Separating user identities from identities used for administrative and other increased access privileges.

   They note this aligns with the HHS' **essential CPG for Separate User and Privileged Accounts** by addressing the separation of privileged or administrator access rights from common user accounts.

3. **Emergency Access Procedure –** Modified to:

   Establish (and implement as needed) written and technical procedures for obtaining necessary electronic protected health information during an emergency.

4. **Automatic logoff –** OCR proposes:

   Deploy technical controls that terminate an electronic session after a predetermined time of inactivity that is reasonable and appropriate.

5. **Log-in attempts [NEW] –** OCR proposes:

   Deploy technical controls that disable or suspend the access of a user or technology asset to relevant electronic information systems after a reasonable and appropriate predetermined number of unsuccessful authentication attempts.

6. **Network segmentation [NEW] –** OCR proposes**:**

   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.

   OCR says this aligns with **HHS' enhanced CPG for Segmentation** because it can help stop an intruder's ability to freely move within a regulated entity's network and protect ePHI.

7. **Data controls [NEW] –** OCR proposes:

   Deploy technical controls to allow access to electronic protected health information only to those users and technology assets that have been granted access rights to the covered entity's or business associate's relevant electronic information systems as specified in § 164.308(a)(10).

8. **Maintenance [NEW] –** OCR proposes:

   Review and test the effectiveness of the procedures and technical controls required by this paragraph (a)(2) at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

B. <u>Encryption and Decryption - Section 164.312(b)(1-3) (pages 221 and 378)</u>

OCR proposes to require encryption and is redesignating the implementation specification for encryption and decryption as a standard. OCR proposes two implementation specifications:

1. *Deploy technical controls to encrypt and decrypt electronic protected health information using encryption that meets prevailing cryptographic standards.*

2. *Encrypt all electronic protected health information at rest and in transit, except to the extent that an exception at paragraph (b)(3) of this section applies.*

OCR also says the adoption of health IT that is certified through the ONC Health IT Certification Program as having the technical capability to encrypt and decrypt electronic health information. Under the proposal, a regulated entity would need to ensure that an encryption solution that it adopts meets prevailing cryptographic standards prior to using it. OCR uses the phrase "prevailing cryptographic standards" to refer to widely accepted standards, but they are not proposing to define this term at this time. Reviewing and testing at least once every 12 months would be required or in response to environmental or operational changes.

OCR proposes the following **exceptions**:

1. Encryption with prevailing cryptographic standards not supported and the covered entity or business associate establishes and implements a written plan to migrate ePHI to a technology asset that supports encryption consistent with a standard that does, within a reasonable and appropriate period of time.
2. An individual requests their ePHI in an unencrypted manner and has been informed of the risks. This exception does not apply where such individual will receive their ePHI pursuant to § 164.524 and the technology used by the individual to receive the ePHI is controlled by the covered entity or its business associate.
3. During an emergency or other occurrence that adversely affects the covered entity's or business associate's relevant electronic information systems in which encryption is infeasible, and the covered entity or business associate implements reasonable and appropriate compensating controls).
4. The technology asset in use is a device under section 201(h) of the Food, Drug, and Cosmetic Act, 21 U.S.C. 321(h) that has been authorized for marketing by the Food and Drug Administration with three exceptions:
    i. A submission received before March 29, 2023, provided that the covered entity or business associate deploys in a timely manner any updates or patches required or recommended by the manufacturer of the device.
    ii. A submission received on or after March 29, 2023, where the device is no longer supported by its manufacturer, provided that the covered entity or business associate has deployed any updates or patches required or recommended by the manufacturer of the device; or
    iii. A submission received on or after March 29, 2023, where the device is supported by its manufacturer.

    NOTE: The above referenced dates refer to devices that fall under the Protecting and Transforming Cyber Health Care (PATCH) Act which was included in the Consolidated Appropriations Act, 2023. For more details on these devices see this FDA webpage.

    OCR says, "We recognize that, to comply with this proposal, some regulated entities may incur costs for replacing legacy medical devices (i.e., medical devices that cannot be reasonably protected against current cybersecurity threats)… By limiting these exceptions to devices that have been updated and/or patched while they were supported by their manufacturer, we believe that this proposal would balance the interest in encouraging regulated entities to dispense with legacy devices with the

cost of replacing such devices. Additionally, the Department believes that regulated entities should already have plans to replace legacy devices that cannot be made cybersecure because of their existing Security Rule obligations."

5. **Alternative measures** – A covered entity or business associate must document in real-time when an exception applies and the compensating controls. When implementing compensating controls they must be reviewed, documented, and signed by the designated Security Official at least once every 12 months or in response to environmental or operational changes, whichever is more frequent.

OCR says their proposal aligns with **HHS' essential CPG for Strong Encryption** by calling for regulated entities to deploy encryption to protect ePHI.

c. Configuration Management - Section 164.312(c)(1) (pages 232 and 380)

OCR proposes a new standard addressing failure to configure technical controls appropriately and calls for deploying technology assets and/or technical controls that protect all of the technology assets in its relevant electronic information systems against malicious software, such as viruses and ransomware in accordance with "covered entity's or business associate's established secure baselines." OCR says that when establishing a baseline (i.e., minimum) level of security for each relevant electronic information system and technology asset, that this baseline should be maintained even when technology changes. Baselines would be determined based on a regulated entity's risk analysis and says, "the baseline for settings that should be applied to the particular asset and similar technologies across the regulated entity's enterprise." OCR proposes five implementation specifications:

1. **Anti-malware protection** - Deploy technology assets and/or technical controls that protect all of the covered entity's or business associate's technology assets.
2. **Software removal** - Remove extraneous software from the covered entity's or business associate's relevant electronic information systems.
3. **Configuration** - Configure and secure operating system(s) and software.
4. **Network ports** - Disable network ports.
5. **Maintenance** - Review and test the effectiveness of the technical controls at least once every 12 months and modify as reasonable and appropriate.

OCR says their proposal aligns with **HHS' enhanced CPG for Configuration Management** which calls for regulated entities to define secure device and system settings, the **enhanced CPG for Detect and Respond to Relevant Threats and Tactics, Techniques, and Procedures** by calling for regulated entities to include malware protection in their security baseline to detect threats and protect electronic information systems, and the **essential CPG for Email Security** which addresses the reduction of risks from email-based threats.

d. Audit Trail and System Log Controls - Section 164.312(d)(1) (page 235 and 381)

OCR proposes to redesignate the standard for audit controls and rename it "audit trail and system log controls." They furthermore call for requiring a regulated entity to deploy either or both technology assets and technical controls that record and identify activity in the regulated entity's relevant electronic information systems. Thus, the proposal would require a regulated entity to record and identify any activity that could present a risk to ePHI, meaning activity in all of its

relevant electronic information systems, not only in its electronic information systems that create, receive, maintain, or transmit ePHI. OCR proposes four implementation specifications under this proposed standard including:

1. **Monitor and identify** - Deploy technology assets and/or technical controls that monitor in real-time all activity in its relevant electronic information systems and identify of unauthorized persons / activity.
2. **Record** - Deploy technology assets / technical controls that record in real-time.
3. **Retain** - Deploy technology assets / technical controls to retain records of all activity.
4. **Scope** - Activity includes creating, accessing, receiving, transmitting, modifying, copying, or deleting ePHI, relevant electronic information systems and its information.

This redesignated standard, as proposed, aligns more closely with **HHS' enhanced CPG for Centralized Log Collection** by addressing the deployment of technical controls to record and identify activity in all electronic information systems.

e. <u>Integrity - Section 164.312(e) (pages 239 and 382)</u>

OCR is proposing to designate and modify the standard as follows:

> *Deploy technical controls to protect electronic protected health information from improper alteration or destruction, both at rest and in transit; and review and test the effectiveness of such technical controls at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.*

OCR states the ONC Health IT Certification Program has the technical capability to verify that the electronically exchanged health information contained within the health IT has not been altered using a hashing algorithm which may contribute to a regulated entity's compliance with the proposed standard for integrity.

f. <u>Authentication - Section 164.312(f)(1) (pages 240 and 382)</u>

OCR proposes to designate and modify the standard to clarify that a regulated entity would be required to deploy technical controls to verify that a technology asset seeking access to the regulated entity's relevant electronic information systems is the one claimed. OCR furthermore proposes four implementation specifications:

1. **Information access management policies** - Deploy technical controls that require users to adopt unique passwords – as well as change default passwords – such that that they are consistent with the current recommendations of authoritative sources.
2. **Multi-factor authentication** -
    a. Deploy MFA to all technology assets to verify that a person seeking access to the relevant electronic information system(s) is the user that the person claims to be.
    b. Deploy MFA for any action that would change a user's privileges in a manner that would alter the user's ability to affect the CIA of ePHI.
    c. **Exceptions** - OCR states, "Because exceptions are a departure from the designed Security Rule framework," they require appropriate review by the Security Official of controls selected by the regulated entity to compensate for the absence of MFA. They state, "Merely because a regulated entity's Security Official has reviewed, approved, and signed off on compensating controls does not mean that those controls are effective.

The regulated entity would also be required to give due consideration to the circumstances surrounding the exception and implement compensating controls effective for those specific circumstances." Regarding the use of compensating controls OCR states, "the Security Official would be required to review the effectiveness of the compensating controls at securing its relevant electronic information systems." Deployment of MFA is NOT required in any of the following circumstances."

1. When a technology asset does not support MFA and there is a written plan to migrate ePHI to a technology asset that supports MFA within a reasonable and appropriate period of time. Accordingly, a regulated entity would be required to establish the plan, implement the plan, and actually migrate ePHI to technology assets that supports MFA within a reasonable and appropriate period of time.
2. During an emergency or other occurrence when MFA is infeasible and the regulated entity can implement compensating controls in accordance with its contingency plan and emergency access procedures.
3. The technology asset in use is a device under section 201(h) of the Food, Drug, and Cosmetic Act, 21 U.S.C. 321(h) that has been authorized for marketing by the Food and Drug Administration under the following circumstances:
    a. For a submission received before March 29, 2023, provided that the covered entity or business associate has deployed any updates or patches required or recommended by the manufacturer of the device.
    b. For a submission received on or after March 29, 2023, where the device is no longer supported by its manufacturer, provided that the covered entity or business associate has deployed any updates or patches required or recommended by the manufacturer of the device.
    c. For a submission received on or after March 29, 2023, where the device is supported by its manufacturer.

    NOTE: The above referenced dates refer to devices that fall under the Protecting and Transforming Cyber Health Care (PATCH) Act which was included in the Consolidated Appropriations Act, 2023. For more details on these devices see this FDA webpage.

    Similar to OCR's proposal related to encryption standards, they acknowledge that some regulated entities will incur costs for replacing legacy devices, "because of the limitations on the proposed exception to MFA where a device was submitted to the FDA for authorization before March 29, 2023 or a device submitted for authorization on or after that date that is no longer supported by its manufacturer…By limiting these exceptions to devices that have been updated and/or patched while they were supported by their manufacturer, we believe that this proposal would balance the interest in encouraging regulated entities to dispense with legacy devices with the cost of replacing such devices."

d. **Alternative Measures** – Where an above exception applies, a covered entity or business associate must document in real-time the existence of an applicable exception and implement reasonable and appropriate compensating controls.

i. **Compensating controls** -
    a. When exception #1 or #2 or #3a or #3b does not apply, the covered entity or business associate must secure its relevant electronic information systems by implementing reasonable and appropriate compensating controls reviewed by the designated Security Official.
    b. When exception #3c applies the covered entity or business associate shall be presumed to have implemented reasonable and appropriate compensating controls where the regulated entity has deployed the security measures prescribed and as instructed by the authorized label for the device, including any updates or patches recommended or required by the manufacturer of the device.
    c. When compensating controls are used they must be reviewed and documented at least once every 12 months.

e. **Maintenance** - Review and test the effectiveness of technical controls at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

OCR states this proposal aligns with deployment of MFA aligns with the Department's essential **CPGs for Email Security and the CPG for Multifactor Authentication** because use of MFA would be applicable to email access and protect assets connected to the internet.

g. Transmission Security - Section 164.312(g) (pages 250 and 384)

A regulated entity is required to implement technical security measures to guard against unauthorized access to ePHI when transmitted electronically, such as through the internet. OCR proposes to redesignate and modify the standard as follows:

> *Deploy technical controls to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network; and review and test the effectiveness of such technical controls at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.*

h. Vulnerability Management - Section 164.312(h)(1) (pages 251 and 384)

OCR is proposing to add a new standard for vulnerability management to address the potential for a bad actor to exploit publicly known vulnerabilities, calling for vulnerability scanning at least every six months. OCR proposes the following four implementation specifications:

1. **Effectiveness** - Review and test effectiveness of the technology asset(s) that conducts the automated vulnerability scans at least once every 12 months.
2. **Monitoring** - Monitor authoritative sources for known vulnerabilities on an ongoing basis and remediate such vulnerabilities.
3. **Penetration testing** - Perform penetration testing of the covered entity's or business associate's relevant electronic information systems by a qualified person at least once every 12 months.
    a. Qualified person defined as "a person with appropriate knowledge of and experience with generally accepted cybersecurity principles and methods for ensuring the confidentiality, integrity, and availability of ePHI."

4. **Patch and update installation** - Deploy technical controls to ensure timely installation of software patches and critical updates as reasonable and appropriate.

OCR states their proposal aligns with HHS' **enhanced CPG for Cybersecurity Testing** and **the CPG for Third Party Vulnerability Disclosure.**

i. Data Backup and Recovery - Section 164.312(i)(1)— (pages 257 and 386)

OCR proposes to add a standard for a new technical safeguard for data backup and recovery to include four implementation specifications:

- **Data backup and recovery** - Deploy technical controls to create and maintain exact retrievable copies of ePHI.
- **Data backup** - Create backups of ePHI with such frequency to ensure retrievable copies of ePHI are no more than 48 hours older than the ePHI maintained in the covered entity or business associate's relevant electronic information systems.
- **Monitor and identify** - Deploy technical controls that, in real-time, monitor, and alert workforce members about any failures and error conditions of the backups.
- **Record** - Deploy technical controls that record the success, failure, and any error conditions of backups.
- **Testing** - Restore a representative sample of ePHI backed up and document the results of such test restorations at least monthly.

j. Information Systems Backup and Recovery - Section 164.312(j) (pages 258 and 386)

OCR proposes to add a new standard for backup and recovery of relevant electronic information systems. Proposed regulatory text below:

> *Deploy technical controls to create and maintain backups of relevant electronic information systems; and review and test the effectiveness of such technical controls at least once every six months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.*

IX. Organizational Requirements - Section 164.314 (pages 262 and 386)

1. Business Associate Contracts or Other Arrangements - Section 164.314(a)(1-2) (pages 262 and 386)

Because OCR believes that regulated entities that in recent years there has a growing number of types of emergencies that require a regulated entity to activate their contingency plan, OCR proposes to add an implementation specification that would require a BAA to include a provision for a business associate to report to the covered entity activation of its contingency plan without unreasonable delay, but no later than 24 hours after activation. Additionally, OCR proposes business associate must also report within 24 hours to a covered entity when they activate their contingency plan. Their proposal does not dictate how this notification should occur. OCR says business associates do not need to alert a covered entities in any designated timeframe for a "basic internet command such as a ping"; only when a commands indicates potential malicious activity.

This proposal would align with HHS' **enhanced CPG for Third Party Incident Reporting** because this proposal would require a business associate to both report to a covered entity or another business

associate activation of its contingency plan within 24 hours of such activation and report known or suspected security incidents.

2. Requirements for Group Health Plans - Section 164.314(b)(1-2) (pages 270 and 370)

OCR proposes to modify the implementation specifications at to address concerns that group health plans may not recognize that reasonable and appropriate safeguarding of ePHI requires the implementation of security measures that are the same as, or at least equivalent to, the security measures in the Security Rule. In other words, OCR is proposing to obligate a plan sponsor or any agent to whom it provides ePHI to implement the administrative, physical, and technical safeguards of the Security Rule.

H. Section 164.316—Documentation Requirements (pages 275 and 388)

OCR proposes to redesignate the implementation specifications for documentation time limits, availability, and updates – such that that a covered entity must do all of the following in writing (full regulatory text on page 388):

- **Written Documentation** - Document the policies and procedures.
- **Retention** - Retain the documentation for 6 years from the date of its creation or the date when it last was in effect, whichever is later.
- **Availability** - Make documentation available to those responsible for implementation.
- **Updates** - Review and update documentation at least once every 12 months and within a reasonable and appropriate period of time after a security measure is modified.

I. Section 164.318—Transition Provisions (pages 280 and 389)

If the provisions of this proposed rule are finalized, all BAA and other agreements will need to be updated. OCR says they understand that regulated entities may be concerned about updating all their BAAs to comply with the new provisions and proposes a transition period to help accommodate this.

OCR proposes that regulated entities can continue to operate under existing BAAs until the earlier of: 1) date the contract is renewed on or after the final rule compliance date; or 2) a year after the effective date. They furthermore propose this transition period would be available when the following conditions are met:

1. Prior to the final rule publication date, the covered entity or business associate had an existing BAA 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.

Compliance with the final rule still applies on the rule's effective date even if a BAA is not yet negotiated. Compliance with the final rule would be required 240 days following its publication in the *Federal Register*.

J. Section 164.320—Severability (pages 285 and 390)

OCR states that if any of the provisions they have proposed are found to be invalid or unenforceable, they will not render the other requirements invalid.

K. New and Emerging Technologies Request for Information (RFI) (page 288)

OCR acknowledges that technology is constantly evolving and cautions regulated entities that before they implement new and emerging technologies, that they must conduct an accurate and thorough assessment to identify risks and vulnerabilities. In this RFI, OCR discusses some examples of new technologies, such as quantum computing, AI, and virtual and augmented reality (VR and AR), and how the Security Rule would apply in each case.

1. Quantum Computing (page 289)

OCR references joint guidance, developed by NIST, CISA, and NSA, which encourages "the early planning for migration to post-quantum cryptographic standards by developing a Quantum-Readiness Road map." It also recommends that organizations prepare a cryptographic inventory, discuss post-quantum roadmaps with technology vendors, consider their supply chain's readiness for quantum computing, and consider the responsibilities of their technology vendors with respect to preparing for quantum readiness. OCR encourages regulated entities to incorporate these activities as part of their ongoing risk management programs – as the steps presented in the joint guidance are all activities that already are required by the administrative safeguards of the updated Security Rule.

2. Artificial Intelligence (page 289)

OCR expects that a regulated entity interested in using AI would include the use of such tools in its risk analyses and associated risk management activities. The regulated entity's risk analysis must include consideration of, among other things, the type and amount of ePHI accessed by the AI tool, to whom the data is disclosed, and to whom the output is provided. OCR states that the "NIST AI Risk Management Framework is a helpful resource for regulated entities to better understand, measure, and manage risks, effects, and harms of AI." Accordingly, as technology such as AI evolves, OCR would expect a regulated entity to perform a risk analysis to consider the effects of such changes on the confidentiality, integrity, and availability of ePHI.

OCR further states they "believe the proposals in this NPRM would clarify our expectations for when and how regulated entities need to consider, prepare for, and address such changes." For example, OCR proposes to expressly require that a regulated entity develop a written inventory of its technology assets. Thus, they would expect that AI software used to create, receive, maintain, or transmit ePHI or that interacts with ePHI, including where ePHI is used to train the AI software, would be listed as part of its technology asset inventory, which feeds into the regulated entity's risk analysis.

Additionally, OCR proposes to require that regulated entities monitor authoritative sources for known vulnerabilities and to remediate such vulnerabilities in accordance with their patch management program. They further propose to require that patches, updates, and upgrades that address critical and high risks be applied promptly. OCR "believes that the adoption of the cybersecurity best practices proposed in this NPRM is an important first step to ensuring that AI tools are deployed by regulated entities in a manner that protects the confidentiality, integrity, and availability of ePHI."

3. Virtual and Augmented Reality (VR and AR) (page 296)

Verification between a regulated entity and a business associate-developer of VR/AR software would be required to ensure that ePHI remains protected to the same extent as it is using other technology assets.

I. Regulatory Impact Analysis (page 299)

OCR identified ten categories of quantifiable costs arising from these proposals that would apply to all regulated entities: 1) conducting a Security Rule compliance audit; 2) obtaining written verification from their business associates or subcontractors that the business associates or subcontractors, respectively, have conducted the required verification of compliance with technical safeguards; 3) notifying other regulated entities when workforce members' access to ePHI is terminated; 4) completing network segmentation; 5) disabling ports and removing extraneous software; 6) deploying MFA; 7) deploying penetration testing; 8) updating policies and procedures; 9) updating workforce training programs; and 10) revising BAAs.

OCR estimates that the first-year costs attributable to this proposed rule total approximately $9 billion. For years two through five, estimated annual costs of approximately $6 billion are attributable to costs of recurring compliance activities.

OCR states, "The cost of complying with the exceptions to encryption and MFA for medical devices authorized by the U.S. Food & Drug Administration for marketing may depend in part on the extent to which a regulated entity relies on legacy devices because the regulated entity may be required to adopt compensating controls. New devices are likely to have encryption and MFA built into them, not requiring compensating controls."

OCR also states that there are many other costs that are not easy to quantify, such as those related to performing an asset inventory. They estimate 822,600 business entities to be impacted by the rule.