F. Section 164.312—Technical Safeguards

1. Current Provisions

Section 164.312 includes five standards for technical safeguards, which are the requirements concerning the implementation of technology and technical policies and procedures to protect the confidentiality, integrity, and availability of ePHI and related information systems. A regulated entity must comply with the standards for technical safeguards in accordance with 45 CFR 164.306(c), the provision that describes the general rules for the security standards.

Under 45 CFR 164.312(a)(1), a regulated entity is required to establish policies and procedures for electronic information systems to allow access only to those persons or software programs that have been granted access rights as specified in 45 CFR 164.308(a)(4). Regulated entities may comply with this standard by implementing a combination of access control methods and technical controls, consistent with the implementation specifications for this standard. The Security Rule does not identify a specific access control method or technology to implement. Regardless of the technology or information system used, access controls should be appropriate for the workforce member's role and/or function.[1] For example, a workforce member responsible for monitoring and administering information systems with ePHI, such as an administrator or a superuser,[2] should only have access to ePHI as appropriate for their role and/or job function.

The implementation specifications that provide instructions for satisfying the access control standard are found at 45 CFR 164.312(a)(2). Two are required and two are addressable.[3] The implementation specifications address unique user identifiers,[4] emergency access

[1] "Security Standards: Technical Safeguards," *supra* note 343, p. 4.

[2] A superuser is "a user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform." NIST definition of "superuser," Glossary, Computer Security Resource Center, National Institute of Standards and Technology, U.S. Department of Commerce, https://csrc.nist.gov/glossary/term/superuser.

[3] *See* 45 CFR 164.306(d) for an explanation of "required" and "addressable" implementation specifications.

[4] 45 CFR 164.312(a)(2)(i).

procedures,[5] automatic logoff,[6] and encryption and decryption.[7] The implementation specification for unique user identification requires a regulated entity to assign unique identifiers to users to facilitate the identification of specific users of an information system.[666] By assigning a unique identifier to each user, a regulated entity can track the specific activity of that user when they are logged into an information system and hold the user accountable for functions they perform in the information system when they access that system.

Under the implementation specification for emergency access procedures, a regulated entity is required to establish procedures, such as documented operational practices and instructions to workforce members, for obtaining access to necessary ePHI during an emergency and to implement such procedures as needed.[8] In accordance with this implementation specification, a regulated entity must identify the types of situations in which its normal procedures for accessing an information system or application that contains ePHI may not work and establish procedures for obtaining access in those situations.[9] These procedures must be established prior to an emergency to instruct workforce members on possible ways to gain access to needed ePHI where, for example, the electrical system has been severely damaged or rendered inoperative, or where a software update fails and prevents the regulated entity from accessing ePHI in its EHR.

The implementation specification for automatic logoff associated with the standard for access control addresses the need for a regulated entity to, when reasonable and appropriate, implement electronic procedures that terminate an electronic session after a period of inactivity.[669] Automatic logoff is an effective way to prevent unauthorized users from accessing

[5] 45 CFR 164.312(a)(2)(ii).
[6] 45 CFR 164.312(a)(2)(iii).
[7] 45 CFR 164.312(a)(2)(iv). [666]
45 CFR 164.312(a)(2)(i).
[8] 45 CFR 164.312(a)(2)(ii).
[9] "Security Standards: Technical Safeguards," *supra* note 343, p. 5. [669]
45 CFR 164.312(a)(2)(iii).

ePHI on a workstation when it is left unattended for a period of time.[10] While many applications have configuration settings that automatically log a user out of the system after a period of inactivity, some systems have more limited capabilities and may activate a screen saver that is password protected.[11]

The implementation specification under the standard for access control addresses encryption and decryption and requires regulated entities, when it is reasonable and appropriate, to implement a mechanism to encrypt and decrypt ePHI.[12] Encrypting data, including ePHI, reduces the likelihood that anyone other than the party that has the key to the encryption algorithm would be able to decrypt (*i.e.*, translate) the data and convert it into plain, comprehensible text.[13]

The standard for audit controls requires a regulated entity to implement hardware, software, and/or procedural mechanisms that record and examine activity in electronic information systems that contain or use ePHI. Most electronic information systems provide some level of audit controls with a reporting method, such as audit reports.[14] These controls are useful for recording and examining information system activity, especially when determining whether a security violation has occurred.[15] The Security Rule does not identify data that must be gathered by the audit controls or how often the audit reports should be reviewed.[16] Instead, a regulated entity must consider its risk analysis and organizational factors, such as current technical infrastructure and hardware and software security capabilities, to determine reasonable and

[10] "Security Standards: Technical Safeguards," *supra* note 343, p. 6.
[11] *Id*.
[12] 45 CFR 164.312(a)(2)(iv).
[13] "Security Standards: Technical Safeguards," *supra* note 343, p. 7.
[14] "Understanding the Importance of Audit Controls," Cybersecurity Newsletter, Office for Civil Rights, U.S. Department of Health and Human Services, p. 1 (Jan. 2017), https://www.hhs.gov/sites/default/files/january-2017cyber-newsletter.pdf?language=es.
[15] *Id.*
[16] *Id.* at 2.

appropriate audit controls for information systems that contain or use ePHI.[17] The audit controls standard has no implementation specifications.

Section 164.312(c)(1), the standard for integrity, requires a regulated entity to implement policies and procedures to protect ePHI from improper alteration or destruction. The integrity of data can be compromised by both technical and non-technical sources. Workforce members or business associates may make accidental or intentional changes that improperly alter or destroy ePHI. Data can also be altered or destroyed without human intervention, such as by electronic media errors or failures.[18] The purpose of this standard is to establish and implement policies and procedures for protecting ePHI from being compromised regardless of the source. Improperly altered or destroyed ePHI can result in clinical quality problems for a covered entity, including patient safety issues.[19]

Section 164.312(c)(2) contains the addressable implementation specification for the integrity standard that requires a regulated entity, when reasonable and appropriate, to implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner. To determine which electronic mechanisms should be implemented to ensure the integrity of ePHI, a regulated entity must consider the various risks to the integrity of ePHI identified during the risk analysis. Once a regulated entity has identified risks to the integrity of its data, it must identify security measures that will reduce the risks.[20]

The standard for person or entity authentication at 45 CFR 164.312(d) requires a regulated entity to establish policies and procedures for verifying that a person seeking access to ePHI is the one claimed. This standard addresses technical controls for ensuring access is allowed only to those persons or software programs that have been granted access rights under

[17] *Id.*
[18] "Security Standards: Technical Safeguards," *supra* note 343, p. 7.
[19] *Id.*
[20] *Id*. at 9.

the administrative safeguard for information access management at 45 CFR 164.308(a)(4). This standard has no implementation specifications.

Under the standard for transmission security at 45 CFR 164.312(e)(1), a regulated entity is required to implement technical security measures to guard against unauthorized access to ePHI when transmitted electronically, such as through the internet. A regulated entity must identify the available and appropriate means to protect ePHI as it is transmitted, select appropriate solutions, and document its decisions.[21]

The two addressable implementation specifications for the transmission security standards are under 45 CFR 164.312(e)(2). The implementation specification for integrity controls requires a regulated entity, when it is reasonable and appropriate, to implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until the ePHI has been disposed.[22] The implementation specification for encryption requires a regulated entity, when it is reasonable and appropriate, to implement a mechanism to encrypt ePHI.

2. Issues To Address

While the intention of 45 CFR 164.312 is for regulated entities to develop and put into place technical controls, the Department is aware that regulated entities have not always achieved the degree of protection for ePHI that we intended. Absent a definition of "implement," some regulated entities might interpret the term to mean something other than implementing technical controls to ensure the confidentiality, integrity, and availability of ePHI. This misinterpretation may leave ePHI partially unprotected because regulated entities may not implement safeguards throughout their enterprise. As discussed above with respect to both the administrative and physical safeguards, the Department is also concerned that regulated entities are not making the connection between the maintenance requirement at 45 CFR 164.306(d) and

[21] *Id*. at 10.

[22] 45 CFR 164.312(e)(2)(i).

the requirement to implement technical safeguards, and therefore, are not reviewing or updating their policies and procedures for technical safeguards. Additionally, the Department believes that regulated entities may not be recognizing that their obligations under the Security Rule to protect ePHI are not limited to protecting electronic information systems that create, receive, maintain, or transmit ePHI, but necessarily include other electronic information systems that affect the confidentiality, integrity, or availability of ePHI.

While the Security Rule relies on a flexible and scalable approach to compliance, the health care industry's shift to a digital environment has substantially increased both the risk to ePHI and the prevalence of technological solutions for addressing those risks. Additionally, the cost of such solutions has, in many cases, decreased over time, as is often the case with technology. For example, when the original Security Rule was published, tools to encrypt ePHI had limited availability, were more costly, and were not user-friendly, particularly for small health care providers.[23] By contrast, in 2024, the technical ability to encrypt data may be seamless in many applications, inexpensive, and widely available in commercial software and hardware products.[24] Where an encryption solution is not integrated into an application, software, or hardware, third-party solutions are often available.[25] Thus, we do not believe that it is appropriate for such provisions to be "addressable."[26]

3. Proposals

[23] 68 FR 8334, 8357 (Feb. 20, 2003).

[24] For example, the ONC Health IT Certification Program requires that certified health IT certified to the end-user device encryption certification criterion at 45 CFR 170.315(d)(7) must encrypt electronic health information stored on end-user devices after use of the technology on those devices stops or prevent electronic health information from being locally stored on end-user devices after use of the technology on those devices stops. *See also* "Security Standards: Technical Safeguards," *supra* note 343, p. 7.

[25] "How to Protect the Data that is Stored on Your Devices," Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security (access July 26, 2024), https://www.cisa.gov/resources-tools/training/howprotect-data-stored-your-devices; *see also* Karen Scarfone, et al., "[Information Technology Laboratory (ITL)] Bulletin: August 2020, Security Considerations for Exchanging Files Over the Internet," National Institute of Standards and Technology, U.S. Department of Commerce (Aug. 2020), https://csrc.nist.gov/files/pubs/shared/itlb/itlbul2020-08.pdf.

[26] 45 CFR 164.306(d).

The Department retains the requirements for technical safeguards generally and proposes additions and modifications to the existing standards and implementation specifications.

a. Section 164.312—Technical Safeguards

The Department proposes to expand the primary provision at 45 CFR 164.312 to clarify that regulated entities as a general matter must implement and document the implementation of technical safeguards adopted for compliance with the Security Rule. This proposal would clarify that the requirement to implement and document technical safeguards would apply to all technical safeguards, including technical controls, implemented by a regulated entity to protect the confidentiality, integrity, and availability of all ePHI it creates, receives, maintains, or transmits.

As noted above, the current provision at 45 CFR 164.312 does not reference the documentation requirements in 45 CFR 164.316. Therefore, for clarity, we propose to explicitly require in 45 CFR 164.312 that documentation of technical safeguards conforms to the requirements in 45 CFR 164.316. This proposed change would clarify that a regulated entity must document the policies and procedures required to comply with this rule and how entities considered the flexibility factors in 45 CFR 164.306(b). It would also clarify that a regulated entity must document each action, activity, and assessment required by the Security Rule. The Department considers the documentation requirements and other provisions of 45 CFR 164.316 to apply to all of the safeguards, including the technical safeguards, and this proposal is intended to remove any potential uncertainty among regulated entities. Additionally, we propose to add maintenance requirements separately to the implementation specifications for particular technical safeguards in 45 CFR 164.312, as discussed below and consistent with our proposals to add similar requirements to particular administrative and physical safeguards.

Additionally, as discussed above, the Department proposes to remove the distinction between required and addressable implementation specifications and make all implementation specifications required, with specific, limited exceptions. Also as discussed above, we propose to modify certain standards and implementation specifications to clarify that the technical safeguards apply to ensure the confidentiality, integrity, and availability of ePHI, which requires a regulated entity to implement the technical safeguards in or on all relevant electronic information systems. These proposals are discussed in greater detail below.

b. Section 164.312(a)(1)—Standard: Access Control

The Department proposes to clarify the standard for access control at 45 CFR 164.312(a)(1) by requiring a regulated entity to deploy technical controls in relevant electronic information systems to allow access only to those users and technology assets that have been granted access rights. This proposed modification would ensure that a regulated entity deploys technical controls, rather than solely ensuring that it implements technical policies and procedures, consistent with our proposals to define "deploy" and "implement."[27] Thus, the proposal would clarify that a regulated entity is not expected to merely establish a policy and procedure, but must also put into place, ensure the operation of, and verify the continued operation of, technical controls for access to its relevant electronic information systems such that the failure to have such technical control in operation throughout its enterprise would be a violation of the new proposed standard. Additionally, the Department's proposal would clarify that access controls would apply to persons with authorized access and to technology assets.

Access controls are one of the key mechanisms by which a regulated entity protects ePHI. Such technical controls ensure that access to the regulated entity's electronic information systems is limited to only users and technology assets that have been granted access rights under the policies and procedures adopted in accordance with the standard for information access management under 45 CFR 164.308.[28] The Security Rule does not identify a specific type of

[27] *See* 45 CFR 164.304 (proposed definitions of "Deploy" and "Implement").

[28] "Security Standards: Technical Safeguards," *supra* note 343, p. 3. [697]
Id. at 4.

access control method or technology to deploy, nor are we proposing to do so in this rule.[697] As discussed above, access rights should be role-based and the technical controls should assist the regulated entity in implementing such policies and procedures. For example, workforce members responsible for monitoring and administering a regulated entity's relevant electronic information systems, such as someone responsible for cybersecurity or providing technical support to users, must only have access to ePHI and to the regulated entity's relevant electronic information systems as appropriate for their role and job function.

We also propose at 45 CFR 164.312(a)(1) to add a paragraph heading to clarify the organization of the regulatory text.

The Department proposes to modify the existing implementation specifications under the standard for access control and to add five new implementation specifications. Additionally, we propose to redesignate the implementation specification for encryption and decryption as a standard.

We propose to modify the implementation specification for unique user identification at 45 CFR 164.312(a)(2)(i) by renaming the implementation specification as "Unique identification" and adding a requirement to assign a unique identifier for tracking each technology asset. These proposed modifications would clarify for regulated entities that the purpose of this requirement is to enable a regulated entity to identify and track unauthorized activity in its relevant electronic information systems. Such unauthorized activity may include activity by unauthorized persons or technology assets. It may also include activity by persons who are authorized to access the regulated entity's relevant information systems but who access ePHI that they do not need to access for their job or function.

The Department also proposes to expand the types of identifiers a regulated entity may assign to users and technology assets beyond names to include numbers and/or other identifiers and to clarify that a unique identifier must be assigned to each user and technology asset in the regulated entity's relevant electronic information systems. This proposed modification would better meet the goals of this implementation specification by requiring a regulated entity to be able to discern and track activities among all users and technology assets, regardless of whether that user or technology asset is a person, hardware, software program, or device. The proposed implementation specification for unique identification aligns with the Department's essential CPG for Unique Credentials, which calls for regulated entities to use unique credentials to help detect and track anomalous activities.[29]

Additionally, we propose to add an implementation specification at proposed 45 CFR 164.312(a)(2)(ii) for administrative and increased access privileges. Access controls should enable an authorized user to access the minimum necessary information needed to perform their job functions.[30] Rights and/or privileges should be granted to authorized users based on the policies and procedures required under the administrative safeguard for information access management.[31] For example, a workforce member who has certain role-based administrative access privileges should have separate user identities for non-administrative access privileges and administrative access privileges. Separating a single workforce member's user identities based on access privilege substantially limits the risk that an intruder will be able to access ePHI through a workforce member's user identity when they are using the administrative access privileges.[32] A regulated entity may be able to improve the control and review of the use of administrative access privileges, such as through a privileged access management system, to understand how privileged accounts are used within its environment and help detect and prevent the misuse of privileged accounts.[33]

[29] "Cybersecurity Performance Goals," *supra* note 18.
[30] *Id*. at 3-4.
[31] *See* 45 CFR 164.308(a)(4) and proposed 45 CFR 164.308(a)(10).
[32] *See* "Controlling Access to ePHI: For Whose Eyes Only?," *supra* note 416.
[33] "Defending Against Common Cyber-Attacks," *supra* note 396.

The proposed implementation specification would require a regulated entity to separate the unique user identities required by the implementation specification for unique user identification based on the type of access privileges used by a specific unique user. For example, the adoption of health IT that is certified through the ONC Health IT Certification Program as having the technical capability to establish user permissions for accessing, and performing actions with, electronic health information based on unique identifiers may contribute to a regulated entity's compliance with the proposed new implementation specification for administrative and increased access privileges, should the proposal be finalized.[34] This proposed new implementation specification aligns with the Department's essential CPG for Separate User and Privileged Accounts by addressing the separation of privileged or administrator access rights from common user accounts.[35]

Additionally, the Department proposes to redesignate the implementation specification for emergency access procedures at 45 CFR 164.312(a)(2)(ii) as proposed 45 CFR 164.312(a)(2)(iii) and to modify it to require a regulated entity to establish both written procedures and technical procedures for obtaining necessary ePHI during an emergency and to implement them as needed. For example, we note that the adoption of health IT that is certified through the ONC Health IT Certification Program as having the technical capability to permit an identified set of users to access electronic health information during an emergency may contribute to a regulated entity's compliance with the proposed implementation specification for emergency access procedures, should the proposal be finalized.[36]

Under the Department's proposal, the implementation specification for automatic logoff at 45 CFR 164.312(a)(2)(iii) would be redesignated as proposed 45 CFR 164.312(a)(2)(iv) and modified to require a regulated entity to deploy technical controls that terminate an electronic

[34] *See* 45 CFR 170.315(d)(1).

[35] "Cybersecurity Performance Goals," *supra* note 18.

[36] *See* 45 CFR 170.315(d)(6).

session after a period of inactivity. Deploying a mechanism to automatically terminate an electronic session after a period of inactivity reduces the risk of unauthorized access when a user forgets or is unable to terminate their session.[37] Failure to deploy automatic logoff not only increases the risk of unauthorized access and potential alteration or destruction of ePHI; it also impedes an organization's ability to properly investigate such unauthorized access because it would appear to originate from an authorized user.[38]

The Department proposes that the period of inactivity be both predetermined and reasonable and appropriate. When determining the length of the period of inactivity, a regulated entity should consider the access privileges of a given user or technology asset, the system(s) being accessed, the environment in which the system access occurs, and other appropriate factors in determining a reasonable and appropriate time of inactivity before session termination. For example, in an emergency setting, a user may not have time to manually log out of a system. User identities with administrative and other high-level access that present a greater risk to the confidentiality, integrity, and availability of ePHI should have appropriately shorter periods of inactivity because of the increased risk. While many applications have configuration settings for automatic logoff,[39] a regulated entity must determine whether the default automatic logoff is reasonable and appropriate and make modifications if it is not. For example, the adoption of health IT that is certified through the ONC Health IT Certification Program as having the technical capability to automatically stop a user's access to health information after inactivity for a predetermined period and require a user to re-enter their credentials to resume or regain access may contribute to a regulated entity's compliance with the proposed implementation specification for automatic logoff, should the proposal be finalized.[40]

[37] "Controlling Access to ePHI: For Whose Eyes Only?," *supra* note 416.

[38] *Id*.

[39] For example, Windows 10 operating system allows users to customize security options to automatically logout a user after a specified period of inactivity.

[40] *See* 45 CFR 170.315(d)(5).

Additionally, we propose to add an implementation specification for log-in attempts at proposed 45 CFR 164.312(a)(2)(v). The proposal would require a regulated entity to deploy technical controls that disable or suspend the access of a user or technology asset to relevant electronic information systems after a certain number of unsuccessful authentication attempts. Although incorrectly keying in a known password by the intended user may occur infrequently, a repeated and persistent failure is a strong indication of an attempt at unauthorized access. For example, brute force attacks are attempts to gain unauthorized access by guessing the password many times in a row.[41] Technical controls that limit the number of incorrect log-in attempts by disabling or suspending the access of a user or technology asset to relevant electronic information systems are appropriate to address unsuccessful login attempts.[42]

The proposal would require a regulated entity to determine the number of unsuccessful authentication attempts that would trigger disabling or suspending access to relevant electronic information system. The number should be reasonable and appropriate for the type of user or technology asset, the electronic information system or technology asset to which access is sought, and the type of information maintained on such information system or technology asset. For example, a regulated entity may determine that any authentication failure of an administrative privileged access account should disable the account because of the level of risk compared to an authentication failure of a non-administrative privileged account. The Department does not propose to define disable or suspend and relies upon the industry understanding that disabling a user's access would require intervention to restore the capability to use the user identity, while a suspension may prevent additional log-in attempts for a temporary, limited period of time.

[41] "Brute Force Attacks Conducted by Cyber Actors," Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security (May. 6, 2020), https://www.cisa.gov/news-events/alerts/2018/03/27/brute-forceattacks-conducted-cyber-actors.

[42] "Security and Privacy Controls for Information Systems and Organizations," *supra* note 600, p. 39.

Consistent with NCVHS' recommendation and existing guidance, the Department also proposes to add an implementation specification for network segmentation at 45 CFR 164.312(a)(2)(vi) that would require a regulated entity to deploy technical controls to segment its relevant electronic information systems in a reasonable and appropriate manner.[43] Under this proposal, a regulated entity with multiple, distinct electronic information systems would be required to separate relevant electronic information systems using reasonable and appropriate technical controls. Network segmentation is a physical or virtual division of a network into multiple segments, creating boundaries between the operational and IT networks to reduce risks, such as threats caused by phishing attacks.[44] For example, where a regulated entity operates both a point-of-sale system and an EHR on the same network, the EHR could be compromised through a successful attack by an intruder moving laterally (*i.e.*, within the same network) from a previously compromised point-of-sale system because the intruder's movements were not impeded by network segmentation. Accordingly, we believe that it is appropriate to require regulated entities to deploy technical controls to segment the networks to which their relevant electronic information systems are connected.[45] What constitutes reasonable and appropriate network segmentation depends on the regulated entity's risk analysis and how it has implemented its network(s) and relevant electronic information systems. This proposed new implementation specification aligns with the Department's enhanced CPG for Network Segmentation because where the CPG is implemented, an intruder's ability to freely move within a regulated entity's network and protect ePHI is minimized.[46]

[43] *See* Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 3 (recommending that the Department require network segmentation as part of a layered security approach, segregating network components based on user characteristics, such as corporate network compared to business associate network); "Layering Network Security Through Segmentation," Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security, https://www.cisa.gov/sites/default/files/publications/layering-network-securitysegmentation_infographic_508_0.pdf; "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients," *supra* note 16, pp. 23 and 31; PR.IR-01, "The NIST Cybersecurity Framework (CSF) 2.0," *supra* note 15.

[44] "Layering Network Security Through Segmentation," *supra* note 712.

[45] Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 3.

[46] "Cybersecurity Performance Goals," *supra* note 18.

The proposed implementation specification for data controls at proposed 45 CFR 164.312(a)(2)(vii) would require a regulated entity to deploy technical controls to allow access to ePHI based on the regulated entity's policies and procedures for granting users and technology assets access relevant electronic information systems as specified in proposed 45 CFR 164.308(a)(10). This implementation specification would require a regulated entity to have in place technical controls that distinguish between users and technology assets, that are permitted to access the regulated entity's relevant electronic information systems and those that are not permitted to do so and would require that the controls permit or disallow access accordingly.

Properly deployed network-based solutions can limit the ability of a hacker to gain access to an organization's network or impede the ability of a hacker already in the network from accessing other electronic information systems—especially systems containing sensitive data.[47] Access controls could include role-based access, user-based access, or any other access control mechanisms the organization deems appropriate.[48] Access controls need not be limited to computer systems—firewalls, network segmentation, and network access control solutions are effective means of limiting access to relevant electronic information systems.[49]

Additionally, we propose to add an implementation specification for maintenance at proposed 45 CFR 164.312(a)(2)(viii). Under this proposal, a regulated entity would be expressly required to review and test the effectiveness of the procedures and technical controls required by the implementation specifications associated with the standard for access control at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

[47] "Controlling Access to ePHI: For Whose Eyes Only?," *supra* note 416.

[48] *Id*.

[49] *Id*.

c. Section 164.312(b)(1)—Standard: Encryption and Decryption

Encryption can reduce the risks and costs of unauthorized access to ePHI.[50] For example, if a hacker gains access to unsecured ePHI on a network server or if a device containing unsecured ePHI is stolen, a breach of PHI will be presumed and reportable under the Breach Notification Rule.[51] The Breach Notification Rule applies to unsecured PHI, which is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance issued under the HITECH Act.[52] The Department's guidance on rendering unsecured PHI unusable, unreadable, or indecipherable to persons who are not authorized to access such PHI states that ePHI at rest (*i.e.*, stored in an information system or electronic media) is considered secured if it is encrypted in a manner consistent with NIST Special Publication 800-111[53] ("SP 800-111"). The ePHI encrypted in a manner consistent with SP 800-111 is not considered unsecured PHI and therefore qualifies for what is commonly known as the Breach Notification safe harbor, meaning that it is not subject to the requirements of the Breach Notification Rule.[54] Thus, by encrypting ePHI in a manner consistent with the Secretary's guidance, a regulated entity may not only fulfill its encryption obligation under the Security Rule, but also make use of the Breach Notification Rule's safe-harbor provision.[55]

As the use of mobile computing devices (*e.g.*, laptops, smartphones, tablets) has become more pervasive, the risks to sensitive data stored on such devices also have increased.[56] And

[50] *Id*.

[51] *See* 45 CFR 402. The presumption applies unless it can be rebutted in accordance with the breach risk assessment described in 45 CFR 164.402(2).

[52] 45 CFR 164.402.

[53] Karen Scarfone, et al., "Guide to Storage Encryption Technologies for End User Devices: Recommendations of the National Institute of Standards and Technology," NIST Special Publication 800-111, National Institute of Standards and Technology, U.S. Department of Commerce (Nov. 2007), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf.

[54] 74 FR 19600, 19009-19010 (Apr. 27, 2009).

[55] 45 CFR 164.402.

[56] "Controlling Access to ePHI: For Whose Eyes Only?," *supra* note 416.

while in 2003 and even in 2013, encryption might have been out of reach for many regulated entities because of cost or a similar reason,[57] today, encryption solutions are generally considered to be widely accessible. The cost of such solutions has decreased significantly, as has the difficulty in implementing such solutions. In fact, many applications have encryption solutions embedded in them.[58] Once enabled, a device's encryption solution can protect stored sensitive data, including ePHI, from unauthorized access in the event the device is lost or stolen. The same is true for most software today.[59] Thus, while encryption of a particular regulated entity's ePHI might not have been reasonable and appropriate in 2003 or 2013, the Department believes encryption generally is reasonable and appropriate today.[60]

Because the prevalence of encryption solutions has increased, as has their affordability and the role they play in protecting information, including ePHI, the Department believes it is appropriate to consider requiring encryption and elevating it from an implementation specification to a standard to increase its visibility and prominence. Based on this and consistent with NCVHS' recommendation, the Department proposes to redesignate the implementation specification for encryption and decryption at 45 CFR 164.312(a)(2)(iv) as a standard at proposed 45 CFR 164.312(b)(1).[61] The proposed standard would incorporate the requirements of two implementation specifications that address encryption—the one addressed here and the one at 45 CFR 164.312(e)(2)(ii).[62] The Department proposes that the new standard would require a regulated entity to configure and implement technical controls to encrypt and decrypt all ePHI in a manner that is consistent with prevailing cryptographic standards. This proposed new standard aligns with the Department's essential CPG for Strong Encryption by calling for regulated

[57] *See* 68 FR 8334, 8357 (Feb. 20, 2003).

[58] "Controlling Access to ePHI: For Whose Eyes Only?," *supra* note 416.

[59] *Id*.

[60] *See* discussion of 45 CFR 164.312, *infra*.

[61] Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 2.

[62] The Department is also proposing to delete the implementation specification for encryption at 45 CFR 164.312(e)(2)(ii) because we are proposing to address the substantive requirements of that implementation specification in proposed 45 CFR 164.312(b)(2).

entities to deploy encryption to protect ePHI and with the recommendation of NCVHS.[63] We also note that the adoption of health IT that is certified through the ONC Health IT Certification Program as having the technical capability to encrypt and decrypt electronic health information, using an encryption algorithm that meets certain requirements, may contribute to a regulated entity's compliance with the proposed standard for encryption and decryption, should the proposal be finalized.[64]

Under the proposal, a regulated entity would need to ensure that an encryption solution that it adopts meets prevailing cryptographic standards prior to using it. The Department uses the phrase "prevailing cryptographic standards" to refer to widely accepted standards for encryption and decryption that are recommended by authoritative sources and that ensure the confidentiality, integrity, and availability of ePHI at the time the regulated entity performs its risk analysis and establishes or modifies its risk management plan. The Department would expect a regulated entity to deploy updated encryption solutions as prevailing cryptographic standards evolve, consistent with both of the proposed requirements discussed above: (1) to review, verify, and update its risk analysis in response to changes in its environment that may affect ePHI; and (2) to review and modify, as reasonable and appropriate, its risk management plan in response to changes in its risk analysis. Thus, a regulated entity using an encryption algorithm that is known to be insecure would not be in compliance with the proposed requirement to deploy an encryption algorithm that meets prevailing cryptographic standards. We are not proposing to define prevailing cryptographic standards in regulatory text at this time.

The Department proposes to add one implementation specification for the proposed standard for encryption and decryption. Specifically, proposed 45 CFR 164.312(b)(2) would

[63] "Cybersecurity Performance Goals," *supra* note 18; Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 2.

[64] *See* 45 CFR 170.315(d)(7) and 170.210(a).

require regulated entities to encrypt all ePHI at rest and in transit, with limited exceptions.[65] Thus, a regulated entity would be required to encrypt all ePHI it maintains, as well as all ePHI it transmits, unless an exception applies, and the following conditions are met:

- Each exception applies only to the ePHI directly affected by the circumstances described in the specific exception.
- Each exception applies only to the extent that the regulated entity documents its understanding that the exception applies to the scenario in which the regulated entity relies upon the exception and why or how the exception applies, and that any additional applicable conditions are met.

The first proposed exception at proposed 45 CFR 164.312(b)(3)(i) would apply to a technology asset currently used by a regulated entity that does not support encryption according to prevailing cryptographic standards. Because the requirements for encryption under the Security Rule today are addressable, a regulated entity may be in compliance with the encryption requirement without actual encryption of ePHI if encryption is not reasonable and appropriate, provided that the entity meets certain conditions. Additionally, technology assets in use today may rely on cryptographic standards that are no longer accepted industry practice. The Department recognizes that it may take some time for a regulated entity to adopt compliant technology assets. Thus, we propose this exception for such technology assets that do not support encryption consistent with prevailing cryptographic standards in limited circumstances. Specifically, to meet this exception, a regulated entity would be required to establish a written plan to migrate ePHI to technology assets that support encryption consistent with prevailing cryptographic standards and to implement such plan. The regulated entity would be required to

[65] For example, adoption of health IT that is certified through the ONC Health IT Certification Program as having the technical capability to encrypt, or prevent the local storage of, electronic health information stored on end-user devices after use of the technology on those devices stops may contribute to a regulated entity's compliance with the proposed implementation specification for encryption and decryption. *See* 45 CFR 170.315(d)(7). Additionally, the

establish and implement the written plan within a reasonable and appropriate period of time. For example, it would not be reasonable or appropriate for a regulated entity to establish a plan to migrate ePHI on a single flash drive within 30 days and not complete migration of that ePHI for a period of a year because migrating ePHI from a flash drive to a more secure medium is a simple and quick process that the regulated entity already determined could be completed within 30 days. Thus, a year would be an unreasonably long period to leave ePHI insufficiently encrypted, particularly after a need to migrate the ePHI has been established. In such circumstances, the regulated entity would not be complying with the requirements of this proposed exception.

The second proposed exception at proposed 45 CFR 164.312(b)(3)(ii) would be available for ePHI transmitted in response to an individual request, pursuant to 45 CFR 164.524, to receive their ePHI in an unencrypted manner. Unencrypted manners for an individual to receive their ePHI may include some types of text messaging, instant messaging, and other applications on a smartphone or another computing device that are capable of making an access request and receiving ePHI.[66] This exception for individual access requests under 45 CFR 164.524 would not apply when the individual would receive their ePHI using technology controlled by the regulated entity, such as a patient portal[736] or other technology for the transmission of ePHI (*e.g.*, API

proposed implementation specification generally is consistent with the Health Data, Technology, and Interoperability: Patient Engagement, Information Sharing, and Public Health Interoperability (HTI-2) NPRM proposal to modify 45 CFR 170.315(d)(7), should it be finalized, to include requirements that authentication credentials be protected using industry-standard encryption and decryption. *See* 89 FR 63536-37, 63778 (Aug. 5, 2024).

[66] Messaging in the context of telehealth is discussed in Department guidance on telehealth. *See* “Guidance on How the HIPAA Rules Permit Covered Health Care Providers and Health Plans to Use Remote Communication Technologies for Audio-Only Telehealth,” Office for Civil Rights, U.S. Department of Health and Human Services (June 13, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-audio-telehealth/index.html.

[736] For example, health IT certified through the ONC Health IT Certification Program as meeting the “[v]iew, download, and transmit to 3rd party” certification criterion must be able to create and transmit continuity of care document summaries to patients through email via an encrypted method of electronic transmission. *See* 45 CFR 170.315(e)(1).

technology).[67] Such email or messaging technologies are considered to be among a covered entity's technology assets because they are components of a covered entity's relevant electronic information systems, and the requirement to encrypt ePHI would apply.

Under the right of access, an individual who is the subject of PHI has the right to inspect and request a copy of PHI about them in a designated record set, subject to certain exceptions. A regulated entity is required to provide such access in the form and format requested by the individual, if it is readily producible in such form and format. Thus, if an individual requests that the regulated entity provide them access in a manner that does not support encryption, a regulated entity is generally required to do so if it does not jeopardize the security of the regulated entity's information systems. For the exception to apply, a regulated entity would be required to have informed the individual of the risks associated with the transmission, receipt, and storage of unencrypted ePHI when the individual requests unencrypted access and to document that the individual has been informed of such risks.[68]

Consistent with the information blocking regulations, the information provided by regulated entities that are also actors must: focus on any current privacy and/or security risks posed by the technology or the third-party developer of the technology; be factually accurate, unbiased, objective, and not unfair or deceptive; and be provided in a non-discriminatory manner.[739] For example, a regulated entity that is an actor must provide information to

[67] The ONC Health IT Certification Program sets forth at 45 CFR 170.550(h) the privacy and security certification framework for Health IT Modules. Section 170.550(h) identifies a mandatory minimum set of the certification criteria that ONC ACBs must ensure are also included as part of specific Health IT Modules that are presented for certification. For example, to meet the "[s]tandardized API for patient and population services" certification criterion, the ONC Health IT Certification Program requires that a Health IT Module presented for testing and certification must demonstrate the ability to establish a secure and trusted connection with an application requesting data for patients. *See* 45 CFR 170.315(g)(10); *see also* 45 CFR 170.215.

[68] *See* "Resource for Health Care Providers on Educating Patients about Privacy and Security Risks to Protected Health Information when Using Remote Communication Technologies for Telehealth," Office for Civil Rights, U.S. Department of Health and Human Services, (Oct. 17, 2023), https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/resource-health-care-providers-educating-patients/index.html. [739] *See* 45 CFR part 171; 85 FR 25642, 25815 (May 1, 2020). [740] *See, e.g.*, 45 CFR part 171.

individuals about the privacy and security risks of all mobile health applications in the same manner.

We are not proposing to require that the documentation be in any particular form or format. Rather, the required information could be on a standard form, chart note, or checkbox, as examples. The Department does not propose to apply this exception to ePHI transmitted in other forms or formats, such as on a CD or other physical device used to maintain and transmit ePHI. The proposal would not absolve a regulated entity from compliance with other applicable laws or regulations, including the information blocking regulations.[740]

We recognize that emergencies or other occurrences may render it infeasible to encrypt ePHI. Thus, the third proposed exception at 45 CFR 164.312(b)(3)(iii) would apply to certain circumstances in which encryption is infeasible. Such circumstances would be limited to when there is emergency or other occurrence that adversely affects a regulated entity's relevant electronic information systems. For the proposed exception to apply, a regulated entity would be required to implement reasonable and appropriate compensating controls in accordance with and determined by its contingency plan.[69] The Department would expect this proposed exception to be applicable for a limited period of time and only when encryption is infeasible. As noted above, the proposed exception to encryption would narrowly apply only when a regulated entity's relevant electronic information system is adversely affected by the emergency or other occurrence. The proposed exception would no longer be applicable at such time encryption becomes feasible, regardless of whether the emergency or other occurrence continues.

The fourth proposed set of exceptions at proposed 45 CFR 164.312(b)(3)(iv) would be for ePHI that is created, received, maintained, or transmitted by a medical device (*i.e.*, a "device" within the meaning of section 201(h) of the Federal Food, Drug, and Cosmetic Act, 21 U.S.C., 321(h)) that is authorized by the FDA for marketing. We propose three separate exceptions for

[69] 45 CFR 164.308(a)(13).

devices that are authorized by the FDA for marketing pursuant to: a submission received before March 29, 2023; a submission received on or after March 29, 2023, where the device is no longer supported by its manufacturer; or a submission received on or after March 29, 2023, where the device is supported by its manufacturer. Where a device has been authorized by the FDA for marketing pursuant to a submission received before March 29, 2023, we propose that the exception at proposed 45 CFR 164.312(b)(3)(iv)(A) would be available only where the regulated entity deploys in a timely manner any updates or patches required or recommended by the manufacturer of the device. We also propose a similar exception at proposed 45 CFR 164.312(b)(3)(iv)(B) for devices authorized by the FDA for marketing pursuant to a submission received on or after March 29, 2023, where the device is no longer supported by its manufacturer, provided that the regulated entity has deployed any updates or patches required or recommended by the manufacturer.

We recognize that, to comply with this proposal, some regulated entities may incur costs for replacing legacy medical devices (*i.e.*, medical devices that cannot be reasonably protected against current cybersecurity threats).[742] We also recognize that legacy devices can pose significant risks to the confidentiality, integrity, and availability of ePHI.[743] By limiting these exceptions to devices that have been updated and/or patched while they were supported by their manufacturer, we believe that this proposal would balance the interest in encouraging regulated entities to dispense with legacy devices with the cost of replacing such devices. Additionally, the Department believes that regulated entities should already have plans to replace legacy devices that cannot be made cybersecure because of their existing Security Rule obligations. We also recognize that at some point, most, if not all, devices will likely become legacy devices and that there may be legitimate reasons not to immediately replace them when the manufacturer ceases to provide support. In such cases, it will continue to be important for regulated entities to plan for how to address their ongoing Security Rule obligations.

Finally, we propose an exception, proposed 45 CFR 164.312(b)(3)(iv)(C), that would be available for a device authorized by the FDA for marketing pursuant to a submission received on or after March 29, 2023, where the device is supported by its manufacturer. We understand that the FDA considers security during the review of medical device marketing submissions, including those for software that is approved as a medical device, and works with device manufacturers to ensure that appropriate cybersecurity protections are built into such devices, pursuant to FDA's authority under the Consolidated Appropriations Act, 2023.[70] Thus, we do not believe it would be necessary or appropriate for the Security Rule to require encryption for an FDA-authorized medical device that has been authorized by the FDA for marketing pursuant to a submission received on or after March 29, 2023 where the device continues to be supported by its manufacturer.

Where a proposed exception applies to the proposed encryption requirement, the Department also proposes to require that a regulated entity implement alternative measures and compensating controls. Specifically, we propose at proposed 45 CFR 164.312(b)(4)(i) to require a regulated entity to document the existence of an applicable exception and implement reasonable and appropriate compensating controls. Under the proposal, we would require documentation to occur in real-time, meaning when the criteria for the exception exist and at the time compensating controls are implemented. For example, a regulated entity disclosing ePHI to

[742] *See* "Next Steps Toward Managing Legacy Medical Device Cybersecurity Risks," MITRE Corporation (Nov. 2023), https://www.mitre.org/sites/default/files/2023-11/PR-23-3695-Managing-Legacy-Medical-Device%20Cybersecurity-Risks.pdf; "Principles and Practices for the Cybersecurity of Legacy Medical Devices," International Medical Device Regulators Forum, p. 8 (Apr. 11, 2023), https://www.imdrf.org/sites/default/files/2023-04/IMDRF%20Principles%20and%20Practices%20of%20Cybersecurity%20for%20%20Legacy%20Medical%20Devices%20Final%20%28N70%29_1.pdf.

[743] "Cybersecurity," U.S. Food & Drug Administration, U.S. Department of Health and Human Services, https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity.

[70] *See* sec. 3305 of Pub. L. 117–328, 126 Stat. 5832 (Dec. 29, 2022) (codified at 21 U.S.C. 360n–2); *see also* "Cybersecurity in Medical Devices Frequently Asked Questions (FAQs)," U.S. Food & Drug Administration, U.S. Department of Health and Human Services, https://www.fda.gov/medical-devices/digital-health-centerexcellence/cybersecurity-medical-devices-frequently-asked-questions-faqs.

an individual by unencrypted email in accordance with the right of access would be required to document in accordance with the proposed 45 CFR 164.312(b)(4)(i) that: (1) before the disclosure, the individual has requested to receive ePHI by unencrypted email or unencrypted messaging technology; and (2) before the disclosure, the regulated entity informed the individual of the risks associated with transmission of unencrypted ePHI. The exception would not apply where such individual requests to receive access to their ePHI pursuant to 45 CFR 164.524 via email or messaging technologies implemented by the covered entity.

At proposed 45 CFR 164.312(b)(4)(i), the Department proposes to require that where a proposed exception applies, a regulated entity would also be required to implement an alternative measure or measures that are reasonable and appropriate compensating controls under proposed 45 CFR 164.312(b)(4)(ii). Compensating controls would be implemented in the place of encryption to protect ePHI from unauthorized access.[71] The Department does not propose to require that compensating controls be limited to technical controls. Rather, a regulated entity should consider the nature of the exception, operating environment, and other appropriate circumstances to determine what controls are reasonable and appropriate and implement compensating controls effective for those circumstances. For example, a regulated entity may use physical access controls, such as physically limiting access to a device, in combination with other controls to compensate for the absence of encryption.

Proposed paragraph (b)(4)(ii)(A) would require that if the regulated entity has determined that an exception applies, it must secure ePHI by implementing reasonable and appropriate compensating controls that are reviewed and approved by the regulated entity's designated

[71] Celia Paulsen, et al., "Glossary of Key Information Security Terms," NIST Interagency and Internal Reports 7298, Revision 3, National Institute of Standards and Technology, U.S. Department of Commerce (July 3, 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf.

Security Official. Because exceptions are a departure from the Security Rule framework, the Department proposes to ensure appropriate focus and review by the Security Official of the controls chosen to compensate for the absence of encryption.

With respect to the exception at proposed 45 CFR 164.312(b)(3)(iv)(C), the Department proposes at paragraph (b)(4)(ii)(B) to presume that a regulated entity had implemented reasonable and appropriate compensating controls where the regulated entity has deployed the security measures prescribed and as instructed by the FDA-authorized label for the device. This would include any updates, including patches recommended or required by the manufacturer of the device. The proposed language recognizes that while the device's label may not specifically require deployment of an encryption solution, it may provide for a specific compensating control and the manner in which that control is to be implemented. While not required, a regulated entity would be permitted to implement additional alternative security measures and compensating controls in accordance with best practices and/or its risk analysis.

Finally, at proposed paragraph (b)(4)(ii)(C), the Department proposes to require that the regulated entity's Security Official review and document the implementation and effectiveness of the compensating controls during any period in which such compensating controls are in use to continue securing ePHI and relevant electronic information systems. While regulated entities should review deployed compensating controls on a routine basis, the Department proposes to require a regulated entity to periodically review the implementation and effectiveness of compensating controls to ensure the continued protection of ePHI.[72] For example, if a regulated entity's plan to migrate ePHI from hardware that does not support encryption changes such that the use of the unencrypted hardware continues for a longer period of time, the regulated entity should review implemented compensating controls to ensure ongoing effectiveness and whether

[72] The Department does not propose to require that the periodic review include a review of whether the conditions of the exception continue to apply because, when the conditions qualifying for an exception change such that an exception no longer applies, a regulated entity would be expected to resume compliance with the standard for encryption and decryption and the associated implementation specifications without exception.

new compensating controls should be deployed. We propose to require the designated Security Office conduct such review at least once every 12 months or in response to environmental or operational changes, whichever is more frequent. Additionally, the Department proposes to require that the review be documented in writing and signed. If the regulated entity's Security Official review determines that certain compensating controls are no longer effective, the Department expects that the regulated entity would adopt new compensating controls that are effective to continue to meet the applicable exception. For example, a regulated entity would be expected to update any compensating controls for use of an FDA-authorized medical device when and as instructed by the manufacturer of the device.

We also propose to add an implementation specification for maintenance at proposed 45 CFR 164.312(b)(5). Under this proposal, a regulated entity would be expressly required to review and test the effectiveness of the technical controls required by the standard for encryption at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate. This proposal is consistent with others in this NPRM that would require regulated entities to maintain specified administrative, physical, and technical safeguards.

d. Section 164.312(c)(1)—Standard: Configuration Management The Department believes that the failure to configure technical controls appropriately and to establish and maintain secure baselines for relevant electronic information systems and technology assets in its relevant electronic information systems presents an opportunity for cyberattack and compromise of ePHI.[73] Accordingly, we propose to add a standard for configuration management at proposed 45 CFR 164.312(c)(1). The proposed standard would require a regulated entity to establish and deploy technical controls for securing relevant electronic information systems and technology assets in its relevant electronic information systems, including workstations, in a

[73] "Defending Against Common Cyber-Attacks," *supra* note 396; *see also* "HIPAA and Cybersecurity Authentication," *supra* note 368.

consistent manner. Under this proposal, a regulated entity also would be required to establish a baseline (*i.e.*, minimum) level of security for each relevant electronic information system and technology asset in its relevant electronic information systems and to maintain such information systems and technology assets according to those secure baselines. Consistent with our proposals regarding risk analysis and risk management planning, the Department intends for a regulated entity to establish its security baseline and to maintain that baseline even when technology changes. For example, a regulated entity that uses software to access ePHI would be required to update the software with patches as reasonable and appropriate. But where a developer ceases to support a software, it would be reasonable and appropriate for the regulated entity to take steps to either replace it or to otherwise ensure that its level of security remains consistent with the regulated entity's established baseline. Under this proposal, if finalized, the Department would expect a regulated entity to continually monitor its relevant electronic information systems and technology assets in its relevant electronic information systems to ensure that the secure baselines established by the regulated entity are maintained and take appropriate actions when a relevant electronic information system or technology asset in a relevant electronic information system fails to meet the established baselines. A regulated entity's secure baselines would be determined based on its risk analysis and use of security settings that are consistent across its relevant electronic information systems and technology assets in its relevant electronic information systems. For example, the risk analysis may determine that a manufacturer's default settings for a particular technology asset are insufficient. Accordingly, the regulated entity may establish the baseline for settings that should be applied to the particular asset and similar technologies across the regulated entity's enterprise. This proposed standard aligns with the Department's enhanced CPG for

Configuration Management, which calls for regulated entities to define secure device and system settings. It also aligns with the enhanced CPG for Detect and Respond to Relevant Threats and Tactics, Techniques, and Procedures by calling for regulated entities to include malware protection in their security baseline to detect threats and protect electronic information systems.[74] Additionally, the proposed standard also aligns with the Department's essential CPG for Email Security, which addresses the reduction of risks from email-based threats.[75]

The Department proposes five implementation specifications for the proposed standard for configuration management.[76] Under the proposed implementation specification for antimalware protection at proposed 45 CFR 164.312(c)(2)(i), a regulated entity would be required to deploy technology assets and/or technical controls that protect all of the technology assets in its relevant electronic information systems against malicious software, such as viruses and ransomware. Anti-malware software, especially when used in combination with other technical controls such as intrusion detection/prevention solutions, can also help prevent, detect, and contain cyberattacks.[77] This protection would be applied to all of a regulated entity's technology assets in its relevant electronic information systems. When determining how to fulfill this proposed obligation, regulated entities may consider deploying tools such as anti-malware and endpoint detection and response (EDR) solutions. Anti-malware tools generally scan a regulated entity's electronic information systems to identify malicious software.[78] Such tools may also quarantine malicious software if identified. As explained by the Office of Management and Budget, "EDR combines real-time continuous monitoring and collection of endpoint data […] with rules-based automated response and analysis capabilities."[79]

[74] "Cybersecurity Performance Goals," *supra* note 18.

[75] *Id*.

[76] *See* proposed 45 CFR 164.312(c)(2).

[77] "What Happened to My Data?: Update on Preventing, Mitigating and Responding to Ransomware," Cybersecurity Newsletter, Office for Civil Rights, U.S. Department of Health and Human Services (Dec. 2019), https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-fall-2019/index.html.

[78] *See* "Understanding Anti-Virus Software," Cybersecurity & Infrastructure Security Agency, U.S. Dept. of Homeland Security (June 30, 2009, rev. Sept. 27, 2019), https://www.cisa.gov/news-events/news/understandinganti-virus-software.

[79] "Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response," M-22-01, Office of Management and Budget, Executive Office of the President, p. 1 (Oct. 8, 2021), https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf.

We propose a new implementation specification for software removal at proposed 45 CFR 164.312(c)(2)(ii) to require a regulated entity to remove extraneous software from the regulated entity's relevant electronic information systems. Software is extraneous if it is unnecessary for the regulated entity's operations. It can be a target for attack, and older applications may no longer be supported with patches for new vulnerabilities.[80] Removal of unnecessary software reduces an avenue of attack. The Department is not proposing to specify what would constitute necessary and unnecessary software. Rather, we intend that the regulated entity would consider removal of unwanted or unused software, for example, default software added by a computer manufacturer or reseller where such software may open an avenue for unnecessary risk because the regulated entity does not intend to use it. Accordingly, the proposal would require a regulated entity to consider all software on its relevant electronic information systems and any potential avenue of risk and address the risk through software removal where such software is unnecessary for the regulated entity's operations.

The proposed implementation specification for configuration at proposed 45 CFR 164.312(c)(2)(iii) would require a regulated entity to configure and secure operating systems and software in a manner consistent with the regulated entity's risk analysis. Generally, a regulated entity's risk analysis should guide its implementation of appropriate technical controls to reduce the risk to ePHI.[81] Requiring operating systems and software to be maintained in a secure manner would reduce exploitable vulnerabilities.[82] Often, known vulnerabilities can be mitigated by applying vendor patches or upgrading to a newer version.[83]

Under the proposed implementation specification for network ports at proposed 45 CFR 164.312(c)(2)(iv), a regulated entity would be required to disable network ports in accordance

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

[81] *Id.*

[82] *Id.*

[83] *Id.*

with the regulated entity's risk analysis.[84] Successful ransomware deployment often depends on the exploitation of technical vulnerabilities such as unsecured ports.[85] The proposal to require network ports to be disabled in accordance with the risk analysis would reduce exploitable vulnerabilities.[86]

Lastly, the proposed implementation specification for maintenance at proposed 45 CFR 164.312(c)(2)(v) would expressly require a regulated entity to review and test the effectiveness of the technical controls required by the other implementation specifications associated with the standard for configuration management at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

e. Section 164.312(d)(1)—Standard: Audit Trail and System Log Controls

Audit controls are crucial technical safeguards that are useful for recording and examining activity in electronic information systems, especially when determining whether a security violation occurred.[87] A regulated entity must consider its risk analysis and organizational factors, such as current technical infrastructure, hardware, and software security capabilities, to determine reasonable and appropriate audit controls.[88] However, based on OCR's enforcement experience, we believe that regulated entities' understanding of and compliance with this standard could be improved by providing more specificity.

Accordingly, the Department proposes to redesignate the standard for audit controls at 45 CFR 164.312(b) as proposed 45 CFR 164.312(d)(1), rename it as the standard for audit trail and system log controls, and to add a paragraph heading to clarify the organization of the regulatory

[84] *See* proposed 45 CFR 164.308(a)(2).

[85] "What Happened to My Data?: Update on Preventing, Mitigating and Responding to Ransomware," *supra* note 751.

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

[87] "Security Standards: Technical Safeguards," *supra* note 343, p. 7.

[88] *Id*.

text. We also propose to modify it to require a regulated entity to deploy either or both technology assets and technical controls that record and identify activity in the regulated entity's relevant electronic information systems. The proposal would replace "procedural mechanisms" with "technical controls," to match the general focus on technical controls in 45 CFR 164.312 and would recognize that a regulated entity may be able to meet the requirements of the standard by deploying either or both technology assets (*e.g.*, software) or technical controls. Under the proposal, a regulated entity would be required to collect sufficient information to understand what a specific activity in its relevant electronic information systems is, such that the regulated entity would be better able to address activity that presents a risk to the confidentiality, integrity, or availability of ePHI. For example, a regulated entity should understand that a given activity in a relevant electronic information system is an attempt to access a portable workstation without authorization. The proposal also would modify the limitation on the regulated entity's obligation to record and identify activity in its relevant electronic information systems. Thus, the proposal would require a regulated entity to record and identify any activity that could present a risk to ePHI, meaning activity in all of its relevant electronic information systems, not only in its electronic information systems that create, receive, maintain, or transmit ePHI. In so doing, the Department would also require a regulated entity to record and identify activity in its electronic information systems that may affect the confidentiality, integrity, or availability of ePHI. This redesignated standard, as proposed, aligns more closely with the Department's enhanced CPG for Centralized Log Collection by addressing the deployment of technical controls to record and identify activity in all electronic information systems.[89] Additionally, as an example, we note that adoption of health IT certified through the ONC Health IT Certification Program may contribute to a regulated entity's compliance with the proposed standard for audit trail and system log

[89] "Cybersecurity Performance Goals," *supra* note 18.

controls where such health IT meets the criteria for auditing actions on health information and recording actions related to electronic health information and audit log status.[90]

The Department proposes four implementation specifications under this proposed standard that are intended to improve the effectiveness of audit controls deployed by a regulated entity. The proposed implementation specification for monitoring and identifying activity at proposed 45 CFR 164.312(d)(2)(i) would require a regulated entity to deploy technology assets and/or technical controls that monitor in real-time (*i.e.*, contemporaneously) all activity occurring in a regulated entity's relevant electronic information systems and identify indications of unauthorized persons and unauthorized activity, as determined by the regulated entity's risk analysis. As proposed, the technology assets and/or technical controls also would be required to alert workforce members of such indications in accordance with the regulated entity's policies and procedures for information system activity review at proposed 45 CFR 164.308(a)(7). Unauthorized activity may include actions by technology assets or persons that have not been authorized to access the regulated entity's ePHI or relevant electronic information systems. It may also include actions by authorized users or technology assets that are inconsistent with the regulated entity's policies and procedures for information access management at proposed 45 CFR 164.308(a)(10). The Department proposes that monitoring be continual and conducted in real-time because asynchronous review would allow for the compromise of ePHI for the period of time between the unauthorized activity and its discovery. OCR's enforcement experience has shown that some regulated entities are potentially failing to implement appropriate audit controls

[90] The criterion for auditing actions on health information requires adoption of health IT that has the technical capability to record actions related to electronic health information; restrict the ability for auditing to be disabled to a limited set of users, if the technology permits; detect whether an audit log has been altered; and not allow actions recorded related to electronic health information to be changed, overwritten, or deleted by technology. *See* 45 CFR 170.315(d)(10); *see* 45 CFR 170.315(d)(2); *see also* 45 CFR 170.210(e).

or to review information system activity in a timely manner, which may have contributed to a reportable breach.[91]

A regulated entity would be required, under the proposed implementation specification for recording activity at proposed 45 CFR 164.312(d)(2)(ii), to deploy technology assets and/or technical controls that record in real-time all activity in the regulated entity's relevant electronic information systems.[766] While technical assets and/or technical controls deployed in accordance with proposed 45 CFR 164.312(d)(2)(i) would monitor activity in its relevant electronic information systems, recording such activity would enable a regulated entity to assess any activity to better understand the activity's effects. The proposed implementation specification at proposed 45 CFR 164.312(d)(2)(iii) would require a regulated entity to deploy technology assets and/or technical controls to retain records of all activity in its relevant electronic information systems as determined by the regulated entity's policies and procedures for information system activity review at 45 CFR 164.308(a)(7)(ii)(A). The proposed implementation specification for scope of activity at proposed 45 CFR 164.312(d)(2)(iv) would clarify what would constitute activity to be monitored and recorded in the regulated entity's relevant electronic information systems as required by the proposed implementation specifications at proposed 45 CFR 164.312(d)(2)(i) and (ii). Specifically, the Department proposes that such activities would include, but would not be limited to, creating, accessing, receiving, transmitting, modifying, copying, or deleting ePHI; and creating, accessing, receiving, transmitting, modifying, copying, or deleting relevant electronic information systems and the information (*i.e.*, not only ePHI) therein.

We also propose to add an implementation specification for maintenance at proposed 45 CFR 164.312(d)(2)(iv). Under this proposal, a regulated entity would be expressly required to review and test the effectiveness of the technology assets and/or technical controls required by

[91] *See, e.g.*, "Montefiore Medical Center," *supra* note 248. [766]
See proposed 45 CFR 164.308(a)(2).

the respective implementation specifications of this section at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

f. Section 164.312(e)—Standard: Integrity

Improper alteration or destruction of ePHI, even unintentionally, can result in clinical quality problems, including patient safety issues, for a covered entity.[92] Workforce members or business associates may make accidental or intentional changes that improperly alter or destroy ePHI.[93] Data can also be altered or destroyed without human intervention, such as by electronic media errors or failures.[94] It is important to protect ePHI from being compromised, regardless of the source.[95]

The current standard for integrity at 45 CFR 164.312(c)(1) requires implementation of policies and procedures, rather than actual deployment of technical controls, to ensure integrity of ePHI. To improve the effectiveness of this standard, the Department proposes to redesignate it as proposed 45 CFR 164.312(e) and modify it for clarity. Under the proposal, a regulated entity would be required to deploy technical controls to protect ePHI from improper alteration or destruction when at rest and in transit and to review and test the effectiveness of such technical controls at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate. For example, the adoption of health IT that is certified through the ONC Health IT Certification Program as having the technical capability to verify that the electronically exchanged health information contained within the health IT has not been altered, using a hashing algorithm that meets certain requirements, may contribute to a regulated entity's compliance with the proposed standard for

[92] "Security Standards: Technical Safeguards," *supra* note 343, p. 8.

[93] *Id*.

[94] *Id*.

[95] *Id*.

integrity.[96] The Department proposes to remove the implementation specification at 45 CFR 164.312(c)(2) because technical controls to corroborate that ePHI has not been altered or destroyed in an unauthorized manner are commonly built into hardware and protocols today. Thus, it is unnecessary to require a regulated entity to specifically deploy such controls.

g. Section 164.312(f)(1)—Standard: Authentication

Authentication ensures that a person is in fact who they claim to be before being allowed access to ePHI by providing proof of identity.[97] The Department proposes to redesignate the standard for person or entity authentication at 45 CFR 164.312(d) as 45 CFR 164.312(f)(1) to rename it "Authentication" to reflect its broad purpose, and to add a paragraph heading to clarify the organization of the regulatory text. Additionally, consistent with our proposals to define "implement" and "deploy," we propose to replace the requirement for a regulated entity to implement procedures with a requirement to deploy technical controls. Also, consistent with our proposals to clarify that a regulated entity's obligations to ensure the confidentiality, integrity, and availability extend to all of its relevant electronic information systems, we propose to clarify that the regulated entity is to deploy technical controls to verify that a person seeking access to the regulated entity's relevant electronic information systems is the one claimed. The Department also proposes to modify the existing standard to clarify that a regulated entity would be required to deploy technical controls to verify that a technology asset seeking access to the regulated entity's relevant electronic information systems is the one claimed. Thus, the proposed standard for authentication would require a regulated entity to deploy technical controls to verify that a person or technology asset seeking access to ePHI and/or the regulated entity's relevant electronic information systems is, in fact, the person or technology asset that the person or asset claims to be. We also propose to remove the reference to an entity because entity is included within the definition of person.

[96] 45 CFR 170.315(d)(8).

[97] "Security Standards: Technical Safeguards," *supra* note 343, p. 9.

The Department proposes four implementation specifications under this standard. Consistent with NCVHS' recommendation to eliminate the use of default passwords, the proposed implementation specification for information access management policies at proposed 45 CFR 164.312(f)(2)(i) would require a regulated entity to deploy technical controls in accordance with its information access management policies and procedures, including technical controls that require users to adopt unique passwords.[98] Among other things, this proposal would ensure that regulated entities change default passwords. Such unique passwords would be required to be consistent with current recommendations of authoritative sources. The Department does not propose to define authoritative sources and defers to best practices for setting and maintaining passwords of sufficient strength to ensure the confidentiality, integrity, and availability of ePHI. Under this proposal, a regulated entity would need to require its workforce members to change any default passwords to unique passwords that are consistent with current authoritative source recommendations for unique passwords, as well as prevent the sharing of passwords among workforce members. Default passwords, typically factory-set passwords, may be discovered in common product documentation and used by attackers to gain access to relevant electronic information systems.[99] Thus, the Department believes that it is crucial for the security of ePHI that a regulated entity eliminate the use of default passwords.

In addition to proposing the elimination of default passwords, the Department proposes a specific requirement for a regulated entity to deploy MFA in the implementation specification for MFA at proposed 45 CFR 164.312(f)(2)(ii). We propose to expressly require MFA, as recommended by NCVHS, because it increases security by ensuring that a compromise of a

[98] Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123, p. 6.

[99] "Risks of Default Passwords on the Internet," Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security (Oct. 7, 2016), https://www.cisa.gov/news-events/alerts/2013/06/24/risks-default-passwordsinternet.

single credential does not allow access to unauthorized users.[100] MFA is an effective way to reduce the risk of brute force attacks and to increase the cost of such attack, making such an attack less appealing to intruders.[101] Further, deployment of MFA aligns with the Department's essential CPGs for Email Security and Multifactor Authentication because use of MFA would be applicable to email access and protect assets connected to the internet.[777] Accordingly, proposed 45 CFR 164.312(f)(2)(ii)(A) would require a regulated entity to deploy MFA to all technology assets in its relevant electronic information systems to verify that the person seeking access to its relevant electronic information system is the user that the person claims to be. A regulated entity should deploy MFA to all technology assets in its relevant electronic information systems in a manner consistent with its risk analysis. MFA allows for the use of different categories of factors as described earlier. A decision by a regulated entity to use specific factors during specific circumstances where MFA is deployed will be dependent upon the risks to ePHI identified by the regulated entity and the ability of technology to use such factors to authenticate specific users. For example, certain behavioral characteristics may not satisfy current standards for MFA; however, the Department anticipates that it may be reasonable and appropriate in the future for a regulated entity to adopt a solution where users provide such characteristics as one of the factors. Additionally, a regulated entity may identify varying levels of risk posed by its technology assets and elect to deploy MFA in different ways to address the risk posed by each asset. For example, consistent with its risk analysis, a regulated entity may choose to deploy a single sign-on (SSO) authentication solution using MFA to allow users to access multiple local applications, while also requiring users to authenticate using MFA to access certain cloud-based services.

This proposed implementation specification generally is consistent with ASTP/ONC's

[100] "Multi-Factor Authentication," Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security (Jan. 5, 2022), https://www.cisa.gov/sites/default/files/publications/MFA-Fact-Sheet-Jan22-508.pdf; Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123, pp. 7-8.

[101] Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123, pp. 7-8.

[777] "Cybersecurity Performance Goals," *supra* note 18.

"Health Data, Technology, and Interoperability: Patient Engagement, Information Sharing, and Public Health Interoperability" (HTI-2) NPRM's proposed revisions to the MFA criterion requiring certified health IT to support authentication, through multiple elements, of the user's identity, according to today's standards such as those recommended by NIST, and enable user to configure, enable, and disable the MFA capabilities.[102] Adoption of health IT that is certified through the ONC Health IT Certification Program as meeting the proposed MFA criterion, should the proposal be finalized, may contribute to a regulated entity's compliance with the proposed implementation specification for MFA in this NPRM.

Under proposed 45 CFR 164.312(f)(2)(ii)(B), a regulated entity would be required to deploy MFA for any action that would change a user's privileges to the regulated entity's relevant electronic information systems in a manner that would alter the user's ability to affect the confidentiality, integrity, or availability of ePHI. These modified privileges may provide a user with a level of access inconsistent with a regulated entity's policies and procedures and increase the risk to ePHI by affording a user who does not need to have access to certain systems or information the opportunity to remove security measures deployed to protect ePHI. Because a user may affect the confidentiality, integrity, or availability of ePHI by accessing a relevant electronic information system, a regulated entity would be expected to deploy MFA for changed privileges in both types of systems.

Similar to the proposed standard for encryption, the Department proposes three exceptions at proposed 45 CFR 164.312(f)(2)(iii) to the proposed specific requirement to implement MFA. The first proposed exception at proposed 45 CFR 164.312(f)(2)(iii)(A) would be for a technology asset that does not support MFA but is currently in use by a regulated entity. Because the requirements for authentication under the existing Security Rule today do not expressly refer to MFA, a regulated entity that is not using MFA to meet the requirement to

[102] *See* 89 FR 63498, 63574, 63506, 63528 (Aug. 5, 2024) (proposed 45 CFR 170.315(d)(13)(ii) of ASTP/ONC's HTI-2 NPRM).

authenticate user identities may argue that it is in compliance with the authentication standard without using MFA. The Department recognizes that it may take some time for a regulated entity to adopt compliant software or hardware, and thus we propose an exception where such software or hardware does not support MFA. To meet this exception, a regulated entity would be required to establish a written plan to migrate ePHI to technology assets that supports MFA and to actually migrate the ePHI to such technology assets in accordance with the written plan. Accordingly, a regulated entity would be required to establish the plan, implement the plan, and actually migrate ePHI to technology assets that supports MFA within a reasonable and appropriate period of time. For example, it would not be reasonable and appropriate for a regulated entity to establish a plan to migrate to a new practice management system that supports MFA and fail to take any steps to perform the migration for an entire year. Applying the standard flexibly and at scale, a reasonable and appropriate timeframe for a system with 5,000 users may be different than one for a solo practitioner; however, both entities would be expected to progress to completion.

We recognize that emergencies or other occurrences may render it infeasible for a regulated entity to use MFA, so we propose a second exception for when MFA is infeasible during an emergency or other occurrence that adversely affects the regulated entity's relevant electronic information systems or the confidentiality, integrity, or availability of ePHI.[103] For the proposed exception to apply, a regulated entity would be required to implement reasonable and appropriate compensating controls in accordance with its contingency plan[104] and emergency access procedures.[105] For example, if an optical scanner used by a regulated entity as one of the required factors for MFA is rendered inoperable (*e.g.*, is temporarily broken or adversely affected by a cyberattack), a compensating control may be to temporarily allow users to log in with their

[103] *See* proposed 45 CFR 164.312(f)(2)(iii)(B).

[104] *See* proposed 45 CFR 164.308(a)(13).

[105] *See* proposed 45 CFR 164.312(a)(2)(iii).

user name and a unique password, rather than with a PIN and retinal scan. The Department would make this proposed exception applicable only for the limited period of time in which MFA is infeasible for the regulated entity during the emergency or other occurrence, regardless of whether the emergency or other occurrence continues.

At proposed 45 CFR 164.312(f)(2)(iii)(C), we propose three exceptions that would be for a technology asset in use that is a device within the meaning of section 201(h) of the Food, Drug, and Cosmetic Act that has been authorized for marketing by the FDA. The first would be for a device authorized by the FDA for marketing pursuant to a submission received before March 29, 2023, while the second would be for a device authorized by the FDA for marketing pursuant to a submission received on or after March 29, 2023, that is no longer supported by its manufacturer. In both cases, the exception would only apply where, the regulated entity has deployed any updates or patches required or recommended by the manufacturer of the device. Similar to our proposal for exceptions to encryption at proposed 45 CFR 164.312(b)(3)(iv)(A) and (B), we recognize that some regulated entities may incur costs of replacing legacy devices because of the limitations on the proposed exception to MFA where a device was submitted to the FDA for authorization before March 29, 2023 or a device submitted for authorization on or after that date that is no longer supported by its manufacturer.[106] However, as discussed above, such devices can pose significant risks to the confidentiality, integrity, and availability of ePHI.[783] By limiting these exceptions to devices that have been updated and/or patched while they were supported by their manufacturer, we believe that this proposal would balance the interest in encouraging regulated entities to dispense with legacy devices with the cost of replacing such devices. Additionally, the Department believes that regulated entities should already have plans to replace legacy devices that cannot be made cybersecure because of their existing Security Rule

[106] *See* "Next Steps Toward Managing Legacy Medical Device Cybersecurity Risks," *supra* note 742; "Principles and Practices for the Cybersecurity of Legacy Medical Devices," *supra* note 742, p. 8. [783] "Cybersecurity," *supra* note 743.

obligations. As discussed above, we also recognize that at some point, most, if not all, devices will likely become legacy devices and that there may be legitimate reasons not to immediately replace them when the manufacturer ceases to provide support. In such cases, it will continue to be important for regulated entities to plan for how to address their ongoing Security Rule obligations.

The third proposed exception to MFA at 45 CFR 164.312(f)(2)(iii)(C)(*3*) for devices authorized by the FDA for marketing would be available for those devices authorized for marketing by the FDA pursuant to a submission received on or after March 29, 2023, where they are supported by their manufacturer. We understand that the FDA considers security during the review of medical device marketing submissions and works with device manufacturers to ensure that appropriate cybersecurity protections are built into such devices, pursuant to FDA's authority under the Consolidated Appropriations Act, 2023.[107] Thus, we do not believe it would be necessary or appropriate for the Security Rule to require MFA for an FDA-authorized medical device that has been authorized by FDA for marketing pursuant to a submission received on or after March 29, 2023, where the device continues to be supported by its manufacturer. However, these devices may continue to be used by a regulated entity when they are no longer supported, consistent with the proposed exception for legacy devices that were approved pursuant to a submission received on or after March 29, 2023, as described above.

Where a proposed exception would apply to the proposed MFA requirement, the Department proposes to require that a regulated entity implement alternative measures and compensating controls.[785] Specifically, when a regulated entity seeks to comply with the Security Rule by meeting one of the proposed exceptions to the proposed MFA requirement, the Department proposes to require a regulated entity to document both the existence of the criteria

[107] *See* sec. 3305 of Pub. L. 117–328, 126 Stat. 5832 (Dec. 29, 2022) (codified at 21 U.S.C. 360n–2); *see also* "Cybersecurity in Medical Devices Frequently Asked Questions (FAQs)," *supra* note 744. [785] Proposed 45 CFR 164.312(f)(2)(iv)(A).

demonstrating that the proposed exception would apply and the rationale for why the proposed exception would apply. Additionally, the proposal would require a regulated entity to implement reasonable and appropriate compensating controls, as described at proposed paragraph (f)(2)(iv)(B).

The proposed requirements for reasonable and appropriate compensating controls are explained under proposed 45 CFR 164.312(f)(2)(iv)(B). Compensating controls are implemented in the place of MFA to protect ePHI.[108] The Department does not propose to require that compensating controls be technical controls. Rather, a regulated entity should consider the nature of the exception, operating environment, and other appropriate circumstances to determine what controls are reasonable and appropriate and implement compensating controls effective for those circumstances. For example, if a software program does not support MFA, deploying a firewall or increasing the sensitivity of an existing firewall protecting that software may in some circumstances constitute a reasonable and appropriate compensating control.[787] In some instances, physical safeguards may serve as reasonable and appropriate compensating controls. For example, limiting access to certain components of a relevant electronic information system to workforce members who meet certain requirements may be a reasonable and appropriate compensating control under some circumstances. In most cases, it would be reasonable and appropriate for a regulated entity to implement multiple compensating controls to ensure that the affected electronic information system is secured.

The Department proposes at proposed 45 CFR 164.312(f)(2)(iv)(B)(*1*) that, to comply with an exception at paragraph (f)(2)(iii)(A) or (B) or (f)(2)(iii)(C)(*1*) or (*2*), the regulated entity would be required to secure the relevant electronic information system with reasonable and appropriate compensating controls that have been reviewed, approved, and signed by the regulated entity's Security Official. Because exceptions are a departure from the designed

[108] "Glossary of Key Information Security Terms," *supra* note 745.
[787] "Securing Your Legacy [System Security]," *supra* note 494.

Security Rule framework, the Department intends to ensure appropriate review by the Security Official of controls selected by the regulated entity to compensate for the absence of MFA. Merely because a regulated entity's Security Official has reviewed, approved, and signed off on compensating controls does not mean that those controls are effective. The regulated entity would also be required to give due consideration to the circumstances surrounding the exception and implement compensating controls effective for those specific circumstances.

With respect to the exception at proposed 45 CFR 164.312(f)(2)(iii)(C)(*3*), the Department proposes at proposed 45 CFR 164.312(f)(2)(iv)(B)(*2*) to presume that a regulated entity had implemented reasonable and appropriate compensating controls where the regulated entity has implemented the security measures prescribed and as instructed by the FDAauthorized label for the device. The proposed language recognizes that while the device's label may not specifically require deployment of an MFA solution, it may provide for a specific compensating control and the manner in which that control is to be implemented. This would include any updates, such as patches, recommended or required by the manufacturer of the device. While not required, a regulated entity would be permitted to implement additional alternative security measures and compensating controls in accordance with best practices and/or its risk analysis.

Additionally, the Department proposes at 45 CFR 164.312(f)(2)(iv)(B)(*3*) that during any period in which compensating controls are in use, the regulated entity's Security Official would be required to review the effectiveness of the compensating controls at securing its relevant electronic information systems. While regulated entities should review implemented compensating controls on a routine basis, the Department intends for a regulated entity to periodically review the implementation and effectiveness of implemented compensating controls to ensure the continued protection of ePHI.[109] For example, if a regulated entity's plan to migrate

[109] The Department does not propose that the periodic review include a review that the conditions of the exception continue to apply because a regulated entity would be expected to resume compliance with the implementation specification of multi-factor authentication when such exception no longer applies.

ePHI from hardware that does not support MFA changes such that the use of the non-MFA hardware continues for a longer period of time, the regulated entity should review implemented compensating controls to ensure ongoing effectiveness and whether new compensating controls should be implemented. We are proposing to require that the review be conducted at least once every 12 months or in response to an environmental or operational change, whichever is more frequent, and that the review be documented. Additionally, the Department proposes to require that the review be documented. If the regulated entity's Security Official review determines that certain compensating controls are no longer effective, the Department would expect the regulated entity to adopt other compensating controls that are effective to continue to meet the applicable proposed exception.

As an example of how proposed 45 CFR 164.312(f)(2)(iii) would operate in concert with proposed 45 CFR 164.312(f)(2)(iv), a regulated entity experiencing an emergency that adversely affects a relevant electronic information system and renders MFA infeasible would be required to document the following:

- The regulated entity has experienced an emergency that has adversely affected a relevant electronic information system, including the nature of the emergency and the specific circumstances that adversely affected the specific electronic information system.
- MFA has been rendered infeasible with respect to the specific relevant electronic information system adversely affected by the emergency.
- The regulated entity has put in place reasonable and appropriate compensating controls in accordance with the regulated entity's emergency access procedures and contingency plan.

As part of its documentation, a regulated entity would need to include the controls that have been deployed, a record of the fact that the compensating controls are in use, and a record indicating that the compensating controls have been reviewed and approved by the regulated entity's

Security Official. Proposed 45 CFR 164.312(f)(2)(iv)(B)(*3*) would require the Security Official to review and document the effectiveness of the compensating controls at least once every 12 months or in response to an environmental or operational change, whichever is more frequent. A determination regarding the effectiveness of the technical controls would be based on their ability to secure the regulated entity's ePHI and its relevant electronic information systems.

Last, we propose to add an implementation specification for maintenance at proposed 45 CFR 164.312(f)(2)(v). Under this proposal, a regulated entity would be expressly required to review and test the effectiveness of the technical controls required by this standard at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

h. Section 164.312(g)—Standard: Transmission Security

Transmission security protects against the interception of ePHI in the communications networks used by regulated entities to transmit ePHI.[110] The Department proposes to redesignate the standard for transmission security as proposed 45 CFR 164.312(g) and to modify the standard consistent with other proposals made elsewhere in this NPRM, as described below. Specifically, we propose to clarify the existing standard by requiring a regulated entity to deploy technical controls to guard against unauthorized access to ePHI in transmission over an electronic communications network. For example, adoption of health IT that is certified through the ONC Health IT Certification Program as having the technical capability to establish a trusted connection using encrypted and integrity message protection or a trusted connection for transport and deploying such capability may contribute to a regulated entity's compliance with the proposed standard for transmission security.[790] These proposed changes are consistent with the Department's proposals to replace "implement" with "deploy" in the context of technical

[110] "Glossary of Key Information Security Terms," *supra* note 745.

[790] *See* 45 CFR 170.315(d)(9).

safeguards to differentiate between implementation of a written policy or procedure and deployment of technical controls.

Consistent with our proposals to require that regulated entities maintain their technical controls, we also propose to require a regulated entity to review and test the effectiveness of its technical controls for guarding against unauthorized access to ePHI that is being transmitted over an electronic communications network. We propose that such review and testing occur at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify such technical controls as reasonable and appropriate.

The Department also proposes to remove the implementation specification for integrity controls at 45 CFR 164.312(e)(2)(i) because these requirements are incorporated in the standard for integrity at proposed 45 CFR 164.312(e), discussed above. A regulated entity would continue to be required to review the current methods used to transmit ePHI and then deploy appropriate solutions to protect ePHI from improper alteration or destruction.[111]

i. Section 164.312(h)(1)—Standard: Vulnerability

Management Hackers can penetrate a regulated entity's network and gain access to ePHI by exploiting publicly known vulnerabilities.[112] Exploitable vulnerabilities can exist in many parts of the technology infrastructure of a regulated entity's relevant electronic information systems (*e.g.*, server, desktop, and mobile device operating systems; application, database, and web software; router, firewall, and other device firmware).[113] A regulated entity can identify technical vulnerabilities in multiple, complementary ways, including:

[111] "Security Standards: Technical Safeguards," *supra* note 343, p. 10-11.

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

[113] *Id*.

- Subscribing to CISA alerts[114] and bulletins.[115]
- Subscribing to alerts from the HHS Health Sector Cybersecurity Coordination Center.[116]
- Participating in an information sharing and analysis center (ISAC) or information sharing and analysis organization (ISAO).
- Implementing a vulnerability management program that includes using a vulnerability scanner to detect vulnerabilities such as obsolete software and missing patches.
- Periodically conducting penetration tests to identify weaknesses that could be exploited by an attacker.

Additionally, CISA has compiled a database of free cybersecurity services and tools, some provided directly by CISA and others provided by private and public sector organizations.[117] For example, public and private critical infrastructure organizations may avail themselves of CISA's Cyber Hygiene Services.[118] These services are available at no cost to such organizations and can help regulated entities reduce their risk level, identify vulnerabilities that could otherwise go unmanaged and increase the accuracy and effectiveness of their response activities, among other benefits, putting them in a better place to make risk-informed decisions. CISA's Cyber Hygiene Services include both vulnerability scanning and web application scanning. CISA also has compiled a specific suite of tools and services for high-risk communities.[119]

To address the potential for a bad actor to exploit publicly known vulnerabilities, and consistent with NCVHS' recommendation, the Department proposes to add a new standard for

[114] *See* "Cybersecurity Alerts & Advisories," Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security, https://www.cisa.gov/news-events/cybersecurity-advisories.

[115] *See* "Bulletins," Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security, https://www.cisa.gov/news-events/bulletins.

[116] *See* "Health Sector Cybersecurity Coordination Center (HC3)," Office of the Chief Information Officer, U.S. Department of Health and Human Services, https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html.

[117] "Free Cybersecurity Services and Tools," *supra* note 313.

[118] "Cyber Hygiene Services," *supra* note 313.

[119] "Cybersecurity Resources for High-Risk Communities," *supra* note 313.

vulnerability management at 45 CFR 164.312(h)(1).[120] The proposed standard would require a regulated entity to deploy technical controls to identify and address technical vulnerabilities in the regulated entity's relevant electronic information systems. The deployment of technical controls should be consistent with the regulated entity's patch management policies and procedures at proposed 45 CFR 164.308(a)(4). This proposed standard aligns with the Department's enhanced CPGs for Cybersecurity Testing and Third Party Vulnerability Disclosure by calling for regulated entities to employ multiple processes to discover technical vulnerabilities, including vulnerabilities in workstations and in technology assets provided by vendors and service providers.[801] For example, a regulated entity should include a device owned by a person other than the regulated entity (*e.g.*, the medical device manufacturer) in its vulnerability management activities where the device is deployed on the regulated entity's network. The regulated entity should also include all workstations (*e.g.*, desktop computers, mobile devices) that are part of its relevant electronic information systems in its vulnerability management activities.

To implement this proposed standard, we propose four implementation specifications. Proposed 45 CFR 164.312(h)(2)(i)(A) would require a regulated entity to conduct automated scans of the regulated entity's relevant electronic information systems, including all of the components of such relevant electronic information systems (*e.g.*, workstations, private networks) to identify technical vulnerabilities. Vulnerability scans detect vulnerabilities such as obsolete software and missing patches.[121] Once identified, assessed, and prioritized, appropriate measures need to be implemented to mitigate these vulnerabilities (*e.g.*, apply patches, harden systems, retire equipment).[122] Under the proposal, the scans would be required to be conducted

[120] Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123, p. 8-9. [801]
"Cybersecurity Performance Goals," *supra* note 18.

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

[122] *Id*.

in accordance with the regulated entity's risk analysis under proposed 45 CFR 164.308(a)(2) and no less frequently than once every six months.

Relatedly, proposed 45 CFR 164.312(h)(2)(i)(B) would add an implementation specification for maintenance of the technology assets that conduct the required automated vulnerability scans. Under this proposal, a regulated entity would be expressly required to review and test the effectiveness of the technology asset(s) that conducts the automated vulnerability scans that would be required by the proposed implementation specification at proposed 45 CFR 164.312(h)(2)(i)(A) at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

Identification of a known vulnerability in a relevant electronic information system or a component thereof is a necessary precursor for a regulated entity to take action to mitigate the vulnerability. A 2019 study on vulnerability and patch management found that 48 percent of respondents reported that their organizations had at least one breach in the preceding two years. Of those, 60 percent said that the breaches could have occurred because an available patch for a known vulnerability had not been applied.[123]

Accordingly, the Department also proposes a new implementation specification for monitoring at proposed 45 CFR 164.312(h)(2)(ii) to require that a regulated entity monitor authoritative sources for known vulnerabilities on an ongoing basis and take action to remediate identified vulnerabilities in accordance with the regulated entity's patch management program.[124] The Department expects such monitoring to be conducted on an ongoing basis and is not proposing to specify a minimum time interval for reviewing sources. We are also not proposing to prescribe the specific sources of known vulnerabilities because such sources may change over

[123] This study is not specific to health care. "Costs and Consequences of Gaps in Vulnerability Response," ServiceNow and Ponemon Institute, p. 3 (2019), https://www.servicenow.com/content/dam/servicenowassets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf.

[124] *See* proposed 45 CFR 164.308(a)(4).

time and the vulnerabilities for which regulated entities may be monitoring may vary greatly among regulated entities. We propose to require that the sources used must be authoritative. Examples of authoritative sources of known vulnerabilities would include NIST's National Vulnerability Database[125] and CISA's Known Exploited Vulnerabilities Catalog.[126]

The proposed implementation specification for penetration testing at 45 CFR 164.312(h)(2)(iii) would require a regulated entity to conduct periodic testing of the regulated entity's relevant electronic information systems for vulnerabilities, commonly referred to as penetration testing. Penetration tests identify vulnerabilities in the security features of an application, system, or network by mimicking real-world attacks[127] and are an effective way to identify weaknesses that could be exploited by an attacker.[809] The proposal would require such testing to be conducted by qualified person(s). We propose to describe a qualified person as a person with appropriate knowledge of and experience with generally accepted cybersecurity principles and methods for ensuring the confidentiality, integrity, and availability of ePHI. We believe that within the cybersecurity industry, it is understood that a person who is qualified to conduct such penetration testing is an individual who has a combination of one or more qualifying credentials, skills, or experiences to perform "ethical hacking" or "offensive security" of information systems. The proposal would require a regulated entity to conduct such testing at least once every 12 months, or in accordance with the regulated entity's risk analysis,[128] whichever is more frequent.

Lastly, we are proposing a new implementation specification for patch and update installation at 45 CFR 164.312(h)(2)(iv) to require a regulated entity to configure and implement technical controls to install software patches and critical updates in a timely manner in

[125] "National Vulnerability Database," *supra* note 398.
[126] "Known Exploited Vulnerabilities Catalog," *supra* note 399.
[127] "Glossary of Key Information Security Terms," *supra* note 745.
[809] "Defending Against Common Cyber-Attacks," *supra* note 396.
[128] *See* proposed 45 CFR 164.308(a)(2).

accordance with the regulated entity's patch management program.[129] The proposed standard for patch management, an administrative safeguard discussed above, would require a regulated entity to establish and implement written policies and procedures for applying patches and updating relevant electronic information system configurations, while this proposal would require the regulated entity to implement technical controls to implement those written policies and procedures. In other words, proposed 45 CFR 164.312(h)(2)(iv) addresses the technical controls to effectuate a regulated entity's patch management plan. Applying patches for technology assets, including workstations, is an effective mechanism to mitigate known vulnerabilities and limit the risk of exploitation.[130] Although older applications or devices may no longer be supported with patches for new vulnerabilities, regulated entities still must take appropriate action if a newly discovered vulnerability affects an older application or device. If an obsolete, unsupported system cannot be upgraded or replaced, additional safeguards should be implemented or existing safeguards enhanced to mitigate known vulnerabilities until upgrade or replacement can occur (*e.g.*, increase access restrictions, remove or restrict network access, disable unnecessary features or services).[131] Deployment of such technical controls would help to ensure that a regulated entity's relevant electronic information systems are updated as quickly as possible after a vulnerability has been identified and a patch released.

The proposed standard for patch management, discussed above, would work in tandem with the proposed standard for vulnerability management to ensure that regulated entities substantially reduce the risk to ePHI from known vulnerabilities.[132] Together, these proposals would clarify that a regulated entity is required to affirmatively seek out information about known vulnerabilities, assess the risks to the confidentiality, integrity, and availability of ePHI, and implement effective mechanisms through both policies and procedures and technical controls

[129] *See* proposed 45 CFR 164.308(a)(5).
[130] "Defending Against Common Cyber-Attacks," *supra* note 396.
[131] *See* "Securing Your Legacy [System Security]," *supra* note 494.
[132] *See* proposed 45 CFR 164.308(a)(5) and 164.312(h)(1).

to reduce the risk, as well the actual occurrence, of breaches resulting from known vulnerabilities. For example, known vulnerabilities should be readily identified by a regulated entity through monitoring of authoritative sources for known vulnerabilities, such as those referenced above, and remediating any identified vulnerabilities. When a vulnerability is discovered, a regulated entity, through its patch management program, should have in place a policy and procedure for applying any available patches or implementing reasonable and appropriate compensating controls if a patch is not available. Remediation may be as simple as applying a vendor-offered software patch or, in the case of software no longer supported by a vendor, designing and implementing reasonable and appropriate compensating controls to reduce the risk of the vulnerability. The policies and procedures required by the proposed standard for patch management in proposed 45 CFR 164.308(a)(4)(i) also would be implemented in part by the proposed implementation specifications associated with the proposed standard for vulnerability management. Those proposed implementation specifications would require the deployment of technical controls to ensure the patch management program is carried out, automated vulnerability scans, and penetration testing, all of which may identify when a patch or compensating control has not been put in place. The Department envisions that the full implementation of all of the proposed standards and implementation specifications would effectively reduce the risk to ePHI.

j. Section 164.312(i)(1)—Standard: Data Backup and Recovery The Security Rule requires regulated entities to regularly create copies of ePHI to ensure that it can be restored in the event of a loss or disruption.[133] However, OCR's enforcement experience indicates that regulated entities could benefit from a more specific standard.

Consistent with the proposed standard for contingency planning at 45 CFR

[133] *See* "Plan A…B…Contingency Plan!," *supra* note 606.

164.308(a)(13)(ii)(B), the Department proposes to add a standard for a new technical safeguard for data backup and recovery. This new standard would require a regulated entity to deploy technical controls to create and maintain exact retrievable copies of ePHI. The proposed changes would remove the existing implementation specification for this activity from the physical safeguards section and place it within technical safeguards. The Department also proposes to modify the language of the existing requirement by removing the limitation that it applies before moving equipment, so that it applies broadly and comprehensively. Elevating data backup and recovery to a standard would also increase the prominence of this requirement and highlight the liability of regulated entities for creating the capacity to restore systems after a data breach.

The Department proposes four new implementation specifications for the data backup and recovery standard. The first, 45 CFR 164.312(i)(2)(i), would require a regulated entity to create copies of ePHI in a manner that ensures that such copies are no more than 48 hours older than the ePHI maintained in the regulated entity's relevant electronic information systems and in accordance with the policies and procedures required by proposed 45 CFR 164.308(a)(13)(ii)(B). The second, 45 CFR 164.312(i)(2)(ii), would require a regulated entity to deploy technical controls that, in real-time, monitor, and alert workforce members about, any failures and error conditions of the backups required by the first implementation specification. The third, 45 CFR 164.312(i)(2)(iii), would require a regulated entity to deploy technical controls that record the success, failure, and any error conditions of backups required. The fourth, 45 CFR 164.312(i)(2)(iv), would require a regulated entity to test the effectiveness of its backups and document the results at least monthly. Specifically, a regulated entity would be required to restore a representative sample of backed up ePHI (after the ePHI is backed up as required by paragraph (i)(2)(i)) and document the results of such test restorations at least monthly. Such tests should include verifying regulated entity's ability to access ePHI from a remote location.

These activities are included in NIST guidance for Security Rule compliance,[134] which directs regulated entities to consider the following questions: Is the frequency of backups appropriate for the environment? Are backup logs reviewed and data restoration tests conducted to ensure the integrity of data backups? Is at least one copy of the data backup stored offline to protect against corruption due to ransomware or other similar attacks? The potential need for these requirements also has been indicated through the rising number of ransomware attacks and the high number of individuals affected in such incidents. The Department believes these new implementation specifications, if finalized, would provide additional instruction for regulated entities about conducting data backups and enhance the ability of regulated entities to avoid costly work stoppages and interruptions in the delivery of health care when data becomes unavailable because of a disaster, security incident, or other emergency. We believe enhanced measures for data backup would reduce the need to pay ransom to hackers to recover compromised data.

k. Section 164.312(j)—Standard: Information Systems Backup and Recovery

The Department also proposes to add a new standard for backup and recovery of relevant electronic information systems at proposed 45 CFR 164.312(j). This proposed standard would require a regulated entity to deploy technical controls to create and maintain backups of relevant electronic information systems. It would also require a regulated entity to review and test the effectiveness of such technical controls at least once every six months or in response to environmental or operational changes, whichever is more frequent, and modify them as reasonable and appropriate. The Department would not require a regulated entity to test every relevant electronic information system; rather, the requirement to test the effectiveness of the

[134] *See* "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide," *supra* note 461, p. 49.

controls would permit a regulated entity to review the relevant log files and to test a representative sample of the backup of its relevant electronic information systems.

This proposed standard would reduce potential gaps in the data that needs to be backed up and recovered, to ensure that regulated entities address compliance across relevant electronic information systems. It is crucial to a regulated entity's recovery from an emergency or other occurrence, including a security incident, that adversely affects its relevant electronic information systems to create and maintain backups of such information systems that comprise the infrastructure that maintains and supports the confidentiality, integrity, and availability of ePHI. The Department would expect that the extent of this activity would be affected by the size and complexity of the relevant electronic information systems used by a regulated entity. It is also consistent with NIST guidance, which directs regulated entities to consider whether backups or images of operating systems, devices, software, and configuration files necessary to support the confidentiality, integrity, and availability of ePHI.[135]

[135] *Id.*