APhA
American Pharmacists Association

March 7, 2025

U.S. Department of Health and Human Services (HHS)
Office for Civil Rights
Attention: HIPAA Security Rule NPRM
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue SW
Washington, DC 20201

RE:[RIN 0945-AA22] HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information

Submitted electronically via www.regulations.gov to Docket No. HHS-OCR-2024-0020

The American Pharmacists Association (APhA) appreciates the opportunity to submit comments on HHS's notice of proposed rule, "HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information." The proposed rule would modify the Security Rule under HIPAA and HITECH to strengthen the rules and standards related to electronic protected health information (ePHI). APhA generally supports the proposals as ways to protect ePHI from cybercrime with specific concerns regarding the breadth, compliance dates, and potential costs of these proposals. Considering all the technologies and equipment within a pharmacy that would be included in the proposed definition of ePHI, APhA asks that HHS extend the compliance date beyond the 180-day statutory minimum, especially for small and rural health care providers. In addition, many of the requirements should be available and maintained by the technology products utilized by covered entities rather than imposing unfunded mandates on covered entities that do not have the resources to comply with these burdensome requirements.

APhA is the only organization advancing the entire pharmacy profession. It represents pharmacists, student pharmacists, and pharmacy technicians in all practice settings, including—but not limited to—community pharmacies, hospitals, long-term care facilities, specialty pharmacies, community health centers, physician offices, ambulatory clinics, managed care organizations, hospice settings, and government facilities. Our

members strive to improve medication use, advance patient care, and enhance public health.

Background

Initially published in 2003, the Security Rule was designed to "protect the privacy and security of individuals' protected health information [], which is individually identifiable health information [] transmitted by or maintained in electronic media or any other form or medium, with certain exceptions."[1] The Security Rule only applies to ePHI. As tools and technologies changed throughout the health care system, HHS has updated and revised the Security Rule, with its most recent revision coming in 2013. HHS notes within the proposed rule that "cybersecurity is a concern that touches nearly every facet of modern health care, certainly more than it did in 2003 or even 2013."[2] HHS specifically mentions "appointment scheduling, prescription orders, telehealth visits, medical devices, patient records, medical and pharmacy claims submissions and billing, insurance coverage verifications, payroll, facilities access and management, internal and external communications, and clinician resources" as areas within health care that require safe and secure technologies, but are also open to cyberattacks, malfunctions, and other security incidents that put at risk the confidentiality, integrity, and availability of ePHI.[3] HHS proposes adopting new rules and standards regarding concerns about the increasing number of cybersecurity incidents and the growing number of individuals affected by these incidents. This is particularly important for pharmacies impacted by the 2024 cyberattack on Change Healthcare. Change Healthcare is a company used by many pharmacies with technology that helps pharmacies know how much to charge consumers at the pharmacy counter. As a result, many pharmacies throughout America could not transmit insurance claims for their patients, resulting in delays in getting prescriptions filled and significant backlogs of prescriptions that pharmacies could not process until a ransom was paid.

Section 160.103 – Definitions (FR 921)

Currently, "the term 'electronic media' encompasses both (1) electronic storage material on which data is or may be electronically recorded; and (2) transmission media used to exchange information already in electronic storage media."[4] This definition "specifically

[1] HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information, 90 Fed. Reg. 921 (Jan. 6, 2025). Available at: https://www.federalregister.gov/d/2024-30983/p-122.
[2] *Id.* at 899. Available at: https://www.federalregister.gov/d/2024-30983/p-130.
[3] *Id.* at 900. Available at: https://www.federalregister.gov/d/2024-30983/p-130.
[4] *Id.* at 921. Available at: https://www.federalregister.gov/d/2024-30983/p-585.

excludes certain transmissions, such as those of paper, via facsimile ("fax"), and voice, via telephone, from being considered transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission."[5] In 2013, when HHS revised the Security Rule, the agency stated "a fax machine accepting a hardcopy document for transmission is not a covered transmission even though the document may have originated from printing from an electronic file."[6] At that same time, HHS "also clarified that ePHI maintained, intentionally or otherwise, in a photocopier, fax machine, or other device is subject to the Security Rule and reminded regulated entities that they should be aware of the capabilities of such devices with respect to their ability to maintain ePHI."[7] HHS further states that technology has changed since 2013 and "[t]he definition of electronic media does not account for these changes because it excepts transmissions via fax, and of voice, via telephone, from transmissions via electronic media, nor does the definition take into consideration new and emerging technologies."[8] As such, HHS proposes to modify the definition of "electronic media" within this proposed rule. HHS proposes to change paragraph 1 of this definition "to clarify that electronic media includes not only media on which data may be recorded, but also media on which data may be maintained or processed."[9] In paragraph 2 of this definition, HHS "propose[s] to revise the description of 'transmission media' to recognize that data is transmitted almost exclusively in electronic form today."[10] HHS suggests that "traditional landlines and fax machines are rapidly being replaced with electronic communication technologies and mobile technologies that use electronic media" and "[t]he Security Rule applies when a regulated entity uses such electronic communication technologies." Additionally, HHS "proposes to replace the term "electronic storage media" with "electronic storage material" in paragraph (2) to clarify the connection between definitions of electronic storage material and transmission media."[11]

APhA seeks clarification on the implications of this definition change, especially regarding regulated entities that utilize traditional landlines and fax machines to transmit ePHI. While APhA supports HHS in implementing the best practices to ensure ePHI is protected, APhA stresses that pharmacies still utilize fax machines daily. Faxes are used in pharmacies for various reasons (filing claims, etc.), but one of the main reasons is that interoperability between electronic health records and pharmacies is

[5] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-585.
[6] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-587.
[7] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-587.
[8] *Id.* at 921-22. Available at: https://www.federalregister.gov/d/2024-30983/p-592.
[9] *Id.* at 922. Available at: https://www.federalregister.gov/d/2024-30983/p-596.
[10] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-601.
[11] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-603.

often nonexistent. Accordingly, if HHS determines an analog option provides viable cyberattack protection, APhA supports HHS maintaining the transmission media description and fax machines as an option for pharmacists to maintain compliance with the proposed Security Rule until interoperability is greatly improved. In addition, pharmacies should be held harmless of any unsecured access to HIPAA-protected information if ePHI is not secured by HHS under this proposed rule.

Section 164.304 – Definitions (FR 922)

Adding a Definition of "Relevant Electronic Information System" (FR 927)

Currently, the "Security Rule includes explicit requirements for regulated entities to protect electronic information systems by implementing policies and procedures to limit physical access to such systems and by implementing technical policies and procedures for electronic information systems that maintain ePHI to allow access to only persons or technology assets that have been granted access rights pursuant to 45 CFR 164.308(a)(4)."[12] The rule goes on to provide that "the physical measures, policies, and procedures that meet the definition of physical safeguards are specifically limited to those that protect regulated entities' electronic information systems and related buildings and equipment."[13] However, it does not explicitly define electronic information systems leading to misunderstanding of the rules related to this subset of technology. Under this proposed rule, HHS "proposes to add a definition of 'electronic information system' to better distinguish the concept from the broader category of an information system."[14]

Under the proposed rule, an electronic information system would be defined as "an interconnected set of information resources under the same direct management control that shares common functionality" and "generally includes technology assets, such as hardware, software, electronic media, information, and data."[15] A relevant electronic information system is defined as "an electronic information system that creates, receives, maintains, or transmits electronic protected health information or that otherwise affects the confidentiality, integrity, or availability of electronic protected health information."[16] HHS notes that "[t]he Security Rule requires a regulated entity to ensure the confidentiality, integrity, and availability of all of the ePHI it creates,

[12] *Id.* at 925. Available at: https://www.federalregister.gov/d/2024-30983/p-644.
[13] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-644.
[14] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-648.
[15] *Id.* at 1011. Available at: https://www.federalregister.gov/d/2024-30983/p-2103.
[16] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-2116.

receives, maintains, or transmits."[17] To do so, "a regulated entity must also protect the electronic information systems that create, receive, maintain, or transmit ePHI and the electronic information systems that otherwise affect the confidentiality, integrity, or availability of ePHI."[18]

APhA acknowledges the importance of health care providers and entities ensuring that ePHI is protected. Further, APhA appreciates that HHS clarifies this point so pharmacists, pharmacies, and other entities can comply with the rules. However, APhA notes that this point of clarification and/or the addition of a new definition will significantly impact pharmacies, given the proposed rule's breadth. HHS uses the example of a payment processing system in the covered entity's gift shop and notes that while it "may not create, receive, maintain, or transmit ePHI, it may affect the confidentiality, integrity, or availability of ePHI in certain circumstances, such as where such systems are connected to the same network as servers that contain ePHI." HHS goes on to state that they would "interpret an electronic information system as otherwise affecting the confidentiality, integrity, or availability of ePHI if it is insufficiently segregated physically and electronically from an electronic information system that creates, receives, maintains, or transmits ePHI or one that otherwise affects the confidentiality, integrity, or availability of ePHI." Considering all the technologies and equipment within a pharmacy that will now be included in this definition, APhA asks that HHS extend the compliance date beyond the 180-day statutory minimum, especially for small and rural health care providers.

Section 164.306 – Security Standards: General Rules (FR 930)

45 CFR 164.306(a)(1) provides that covered entities and business associates must "[e]nsure the confidentiality, integrity, and availability of all ePHI the regulated entity creates, receives, maintains, or transmits."[19] In this proposed rule, HHS makes it apparent that the requirements of the Security Rule apply to all ePHI, not just some. APhA supports HHS in providing increased guidance so pharmacies, pharmacists, and other health care entities can better comply with the rules. APhA also favors HHS's efforts to utilize consistent language throughout the rules to make them easier for practitioners to read and understand.

[17] *Id.* at 927. Available at: https://www.federalregister.gov/d/2024-30983/p-681.
[18] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-681.
[19] *Id.* at 930. Available at: https://www.federalregister.gov/d/2024-30983/p-747.

Regarding flexibility and scalability, APhA appreciates HHS's intent "to preserve those elements to the extent possible."[20] APhA understands the importance of "deploy[ing] strong security measures to protect ePHI and related information systems" to combat cyberattacks but asks HHS to keep these new proposals' implications on small and rural health centers front of mind.[21] These new proposals will cost these entities, especially independent pharmacies, significant money and resources at a time when pharmacies are struggling to remain open. Since 2020, more than 2,200 community pharmacies have closed.[22] To offset some of these costs, APhA proposes that HHS offer incentives or cover the costs of implementing these changes to ensure that small and rural health centers, including pharmacies, can quickly and fully comply with this rule while still serving as health care hubs for their communities. At a minimum, APhA asks HHS asks that HHS extend the compliance date beyond the statutory minimum of 180 days. Documentation, reviews, and audits – may be labor and cost-intensive.

Section 164.308 – Administrative Safeguards (FR 934)

45 CFR 164.308 outlines the administrative safeguards that regulated entities, including pharmacists and pharmacies, must implement and follow. APhA acknowledges that regulated entities must abide by all these proposed provisions if the rule becomes final. Therefore, APhA supports HHS extending the compliance date beyond the statutory minimum of 180 days after the effective date. Additionally, APhA asks HHS to remove any proposed rules or standards that are duplicative so as not to overburden regulated entities implementing these changes.

Section 164.308(a)(1)(i) – Standard: Technology Asset Inventory (FR 936)

HHS proposes a new standard for the security management process via 45 CFR 164.308(a)(1)(i). This standard "would require a regulated entity to conduct and maintain an accurate and thorough written technology asset inventory and a network map of its electronic information systems and all technology assets that may affect the confidentiality, integrity, or availability of ePHI."[23] As such, entities would be required to "identify its information systems that create, receive, maintain, or transmit ePHI and all technology assets, as [HHS] propose[s] to define them in 45 CFR 164.304, that may

[20] *Id.* at 931. Available at: https://www.federalregister.gov/d/2024-30983/p-761.
[21] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-761.
[22] Local Pharmacies on the Brink, New Survey Reveals. National Community Pharmacists Association (Feb. 27, 2024). Available at: https://ncpa.org/newsroom/news-releases/2024/02/27/local-pharmacies-brink-new-survey-reveals.
[23] HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information, 90 Fed. Reg. 937 (Jan. 6, 2025). Available at: https://www.federalregister.gov/d/2024-30983/p-852.

affect ePHI in such information systems in order to secure them."[24] HHS reasons that "[r]egulated entities cannot understand the risks to the confidentiality, integrity, and availability of their ePHI without a complete understanding of these assets."[25]

More specifically, under "proposed 45 CFR 164.308(a)(1)(ii)(A), the regulated entity would be required to establish a written inventory that contains the regulated entity's technology assets."[26] "[P]roposed 45 CFR 164.308(a)(1)(ii)(B) would require a regulated entity to develop a network map that illustrates the movement of ePHI throughout its electronic information systems, including but not limited to how ePHI enters and exits such information systems, and is accessed from outside of such information systems."[27] "[A] regulated entity would be required to review and update the written inventory of technology assets and the network map in the following circumstances: (1) on an ongoing basis, but at least once every 12 months; and (2) when there is a change in the regulated entity's environment or operations that may affect ePHI" under 45 CFR 164.308(a)(1)(ii)(C).[28]

APhA appreciates that HHS provides more specificity regarding these requirements so that pharmacists, pharmacies, and other health care entities can ensure that they follow these policies. APhA acknowledges the reasoning of HHS's proposal to require written technology asset inventories and network maps. However, APhA is concerned about the resources and costs of creating these two documents for many entities, especially small and rural health care entities. Again, APhA encourages HHS to provide incentives or funding for entities to create and maintain technology asset inventories and network maps, especially for small and rural health care entities, before imposing an unfunded mandate. At a minimum, APhA asks that HHS delay this policy's implementation and compliance date to ensure regulated entities can comply with its requirements. This additional time may be critical to small and rural health care entities. Additionally, APhA asks that HHS provide an example of a network map to educate those tasked with creating them for the health care entity.

Section 164.308(a)(2)(i) – Standard: Risk Analysis (FR 938)

HHS provides that "[c]onducting a risk analysis is necessary to adequately protect the confidentiality, integrity, and availability of ePHI because it provides the basis for

[24] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-852.
[25] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-852.
[26] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-864.
[27] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-867.
[28] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-868.

determining the manner in which the regulated entity will comply with and carry out the other standards and implementation specifications in the Security Rule."[29] Within this proposed rule, HHS outlines the eight minimum implementation specifications for performing and documenting a risk analysis.[30] The first specification states, "Review the technology asset inventory and the network map to identify where ePHI may be created, received, maintained, or transmitted within its information systems."[31] APhA asks that HHS provide further instruction and guidance on these eight implementation specifications. Additionally, APhA reiterates its above points regarding the creation of unfunded mandates for technology asset inventories and network maps.

Section 164.308(a)(4)(i) – Standard: Patch Management (FR 942)

HHS states"[m]any cyberattacks could be prevented or substantially mitigated if regulated entities implemented activities to manage the implementation of patches, updates, and upgrades to comply with the Security Rule's requirements for risk management, which can deter one of the common types of attacks: exploitation of known vulnerabilities."[32] Accordingly, HHS "proposes six implementation specifications at proposed 45 CFR 164.308(a)(4)(ii) that would be associated with the proposed standard for patch management."[33] Regulated entities would be required "to establish written policies and procedures for identifying, prioritizing, acquiring, installing, evaluating, and verifying the timely installation of patches, updates, and upgrades throughout its electronic information systems that create, receive, maintain, or transmit ePHI or that otherwise affect the confidentiality, integrity, or availability of ePHI."[34] The proposed rule requires these policies and procedures to be reviewed at least once every 12 months, with the regulated entity making any needed modifications following this review.[35] Further, "the proposed implementation specification for application at proposed paragraph (a)(4)(ii)(C) would require a regulated entity to patch, update, and upgrade the configurations of its relevant electronic information systems in accordance with its written policies and procedures and based on the results of: the regulated entity's risk analysis that would be required by proposed 45 CFR 164.308(a)(2), the vulnerability scans that would be required under proposed 45 CFR 164.312(h)(2)(i), the monitoring of authoritative sources that would be required under

[29] *Id.* at 938. Available at: https://www.federalregister.gov/d/2024-30983/p-880.
[30] *Id.* at 941. Available at: https://www.federalregister.gov/d/2024-30983/p-927.
[31] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-929.
[32] *Id.* at 942. Available at: https://www.federalregister.gov/d/2024-30983/p-958.
[33] *Id.* at 943. Available at: https://www.federalregister.gov/d/2024-30983/p-970.
[34] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-970.
[35] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-970.

proposed 45 CFR 164.312(h)(2)(ii), and penetration tests proposed at 45 CFR 164.312(h)(2)(iii)."[36]

APhA acknowledges the risks and vulnerabilities that older technologies and devices may present and recognizes the need for regulated entities to implement patches and updates to comply with the Security Rule and protect ePHI. APhA asks HHS to provide further guidance on this proposal and extend the compliance date beyond the suggested 180 days from the effective date to ensure that entities can adjust to these changes. This extension is critical for small and rural health care providers, who may not have an information technology team or resources to implement these changes immediately. Further, APhA notes that the costs of creating and monitoring these policies could be significant for some health care entities, including pharmacies. As such, APhA reiterates that incentives and funding for these changes could help ensure implementation is more swiftly adopted without financially burdening already struggling entities.

Section 164.308(A)(7)(I) – Standard: Information System Activity Review (FR 946)

HHS notes within the proposed rule that "[d]etecting and preventing data leakage initiated by malicious authorized users is a significant challenge" and cites examples of employees and business associates who have infiltrated systems housing ePHI.[37] Because of this, HHS has suggested that there are compliance challenges regarding the information system activity review standard and has proposed five implementation specifications for this standard. One of "[t]he proposed implementation specification for policies and procedures at proposed 45 CFR 164.308(a)(7)(ii)(A) would require a regulated entity to establish written policies and procedures for retaining and reviewing records of activity in the regulated entity's relevant electronic information systems by persons and technology assets."[38] This review would require regulated entities to review, at a minimum, "audit trails, event logs, firewall logs, system logs, data backup logs, access reports, anti-malware logs, and security incident tracking reports" under 45 CFR 164.308(a)(7)(ii)(B).[39] HHS suggests that larger regulated entities utilize an automated solution that sends real-time alerts.[40] In contrast, HHS advises smaller regulated entities to "have designated staff that manually review log files and audit trials multiple times per week."[41]

---

[36] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-970.
[37] *Id.* at 946. Available at: https://www.federalregister.gov/d/2024-30983/p-1040.
[38] *Id.* at 947. Available at: https://www.federalregister.gov/d/2024-30983/p-1048.
[39] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1048.
[40] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1050.
[41] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1050.

APhA recognizes the importance of reviewing information system activity to prevent unauthorized access and other use of inappropriately viewed ePHI. Regarding this rule, APhA shares the same concerns stated above – implementing these changes will be labor- and significantly cost-intensive, especially for small and rural health care providers. APhA echoes that incentives and funding for implementing these changes will result in more prompt compliance.

Section 164.308(A)(9)(I) – Standard: Workforce Security (FR 948)

Within this proposed rule, HHS provides that "[d]ata breaches caused by current and former workforce members are a recurring issue."[42] HHS states that "[e]ffective identity and access management policies and controls are essential to reduce the risks posed by these types of insider threats."[43] To provide clarity and ensure regulated entities remain compliant with this standard, HHS "proposes to redesignate the workforce security standard at 45 CFR 164.308(a)(3)(i) as proposed 45 CFR 164.308(a)(9)(i), to add a paragraph heading to clarify the organization of the regulatory text, and to modify the regulatory text [to] clarify that a regulated entity must implement written policies and procedures ensuring that workforce members have appropriate access to ePHI and to relevant electronic information systems."[44] The proposed standard also requires a regulated entity to have written procedures for the termination of this access, including a clause that provides "the workforce member's access be terminated as soon as possible, but no later than one hour after the workforce member's employment or other arrangement ends."[45]

APhA generally supports the proposed standard regarding workforce security, as it ensures the ongoing protection of ePHI. APhA is concerned about the one-hour rule regarding termination of access, as this may not be feasible in all circumstances.

Section 164.308(A)(11)(I) – Standard: Security Awareness Training (FR 952)

HHS states, "[a] covered entity's workforce is its frontline not only in patient care and patient service[] but also in safeguarding the privacy and security of PHI."[46] As such, HHS's "proposed standard would require a regulated entity to implement security

[42] *Id.* at 949. Available at: https://www.federalregister.gov/d/2024-30983/p-1074.
[43] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1074.
[44] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1084.
[45] *Id.* at 950. Available at: https://www.federalregister.gov/d/2024-30983/p-1084.
[46] *Id.* at 952. Available at: https://www.federalregister.gov/d/2024-30983/p-1120.

awareness training for all workforce members on protection of ePHI and information systems as necessary and appropriate for the members of the workforce to carry out their assigned function(s) (*i.e.*, role-based training)."[47] HHS provides that "under this proposal, workforce members would receive security awareness training on the protection of ePHI and on the regulated entity's Security Rule policies and procedures that is based on their specific role at least once a year."[48] This proposal also outlines requirements for training new hires and requires regulated entities to provide ongoing education to workforce members regarding security responsibilities and notices of any relevant threats.[49]

APhA supports employees receiving ongoing training from regulated entities regarding patient data protection, best practices, and cybersecurity standards. APhA asks HHS to continue to allow regulated entities to implement this training and not overburden them with repetitive or trivial training. Further, APhA asks for additional guidance on what constitutes ongoing education to ensure entities can comply with these updates to this standard.

Section 164.308(A)(13)(I) – Standard: Contingency Plan (FR 954)

HHS notes that "[c]ontingency plans are critical to protecting the availability, integrity, and security of data during unexpected adverse events."[50] The proposed standard "would require a regulated entity to establish (and implement as needed) a written contingency plan, consisting of written policies and procedures for responding to an emergency or other occurrence, including, but not limited to, fire, vandalism, system failure, natural disaster, or security incident, that adversely affects relevant electronic information systems."[51] This standard also "clarif[ies] that the procedures to create and maintain exact retrievable copies of ePHI must be in writing[] and … such procedures [] include verifying that the ePHI has been copied accurately."[52] APhA acknowledges the importance of contingency plans in ensuring that health care entities can quickly resume normal operations following an unforeseen event. APhA repeats its concerns regarding the costs and resources of complying with these additional standards within the suggested 180 days following the rule becoming effective.

---

[47] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1129.
[48] *Id.* at 953. Available at: https://www.federalregister.gov/d/2024-30983/p-1139.
[49] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1144.
[50] *Id.* at 954. Available at: https://www.federalregister.gov/d/2024-30983/p-1172.
[51] *Id.* at 955. Available at: https://www.federalregister.gov/d/2024-30983/p-1178.
[52] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1181.

Section 164.308(b) (FR 935)

Under 45 CFR 164.308(b)(1), "a covered entity [can] engage a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf when it obtains satisfactory assurances (consistent with the organizational requirements for business associate agreements or other arrangements in 45 CFR 164.314(a)) that the business associate will appropriately safeguard the ePHI."[53] 45 CFR 164.308(b)(2) provides that "a business associate may retain a subcontractor to create, receive, maintain, or transmit ePHI on its behalf if the business associate obtains satisfactory assurances through a business associate agreement or other arrangement that the subcontractor will appropriately safeguard the information."[54] Further, 45 CFR "164.308(b)(3) requires that the contract or other arrangement be in writing."[55] Within this proposed rule, HHS "proposes several modifications to the Security Rule to provide greater assurance that business associates and their subcontractors are protecting ePHI because a subcontractor to a business associate is also a business associate."[56]

APhA supports health care providers and entities adopting best practices to ensure that ePHI is protected and shared through various organizations. However, APhA encourages HHS to ensure that any new requirements do not overburden regulated entities with unnecessary forms, verifications, or procedures.

Section 164.310 – Physical Safeguards (FR 957)

HHS provides that "the physical safeguards standards address the essential requirements for regulated entities to apply to limit physical access to their relevant electronic information systems to only authorized workforce members."[57] Currently, four standards comprise the Security Rule's physical safeguards, which are required by 45 CFR 164.306 and codified in 45 CFR 164.310.[58] Conforming with 45 CFR 164.306(c), "[t]hese standards require regulated entities to implement physical safeguards for facility access controls, workstation use, workstation security, and device and media controls."[59] HHS proposes to retain these four standards while proposing some modifications to 45 CFR 164.306.[60]

---

[53] *Id.* at 935. Available at: https://www.federalregister.gov/d/2024-30983/p-837.
[54] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-837.
[55] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-837.
[56] *Id.* at 956. Available at: https://www.federalregister.gov/d/2024-30983/p-1195.
[57] *Id.* at 958. Available at: https://www.federalregister.gov/d/2024-30983/p-1245.
[58] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1274.
[59] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1248.
[60] *Id.* at 959. Available at: https://www.federalregister.gov/d/2024-30983/p-1274.

HHS "proposes to expand the introductory language at 45 CFR 164.31 to clarify that the Security Rule requires that physical safeguards be applied to all ePHI in the possession of the regulated entity, that is, throughout the regulated entity's facilities."[61] Additionally, HHS "proposes to modify all four physical safeguard standards to require that the requisite policies and procedures be in writing and implemented throughout the enterprise."[62] HHS's proposal also includes reviewing and testing these measures at least once every 12 months.[63] Looking at 45 CFR 164.310(a)(1), HHS "proposes to modify the standard for facility access controls … to clarify that the policies and procedures required by this standard must be in writing and address physical access to all of a regulated entity's relevant electronic information systems and the facility or facilities in which these systems are housed and to add a paragraph to clarify the organization of the regulatory text."[64] The proposal would also require regulated entities to review and test these policies and procedures at least once every 12 months.[65] Regarding 45 CFR 164.310(b) (redesignated as proposed 45 CFR 164.310(b) and (c)), HHS "proposes to modify the standard for workstation use to clarify that policies and procedures established by a regulated entity to govern the use of workstations be in writing and address all workstations that access ePHI or the regulated entity's relevant electronic information systems."[66] HHS states that implementing these specific changes aims to "recognize the increasingly mobile nature of ePHI and workstations that connect to the information systems of regulated entities."[67] The proposed standards also require these written policies and procedures to be reviewed and tested at least once every 12 months.[68] With respect to 45 CFR 164.31(d)(1), HHS proposes the regulated entities have "written policies and procedures that govern the receipt and removal of technology assets that maintain ePHI into and out of a facility, and the movement of these assets within the facility, [that] include tracking relevant information in the technology asset inventory."[69] Again, the proposed rules require that these written policies and procedures be reviewed and tested at least once every 12 months.[70]

APhA generally supports the proposed modifications related to physical safeguards outlined within this proposed rule. APhA notes that each of the modifications described

---

[61] *Id.* at 959-60. Available at: https://www.federalregister.gov/d/2024-30983/p-1275.
[62] *Id.* at 960. Available at: https://www.federalregister.gov/d/2024-30983/p-1276.
[63] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1276.
[64] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1279.
[65] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1283.
[66] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1284.
[67] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1284.
[68] *Id.* at 961. Available at: https://www.federalregister.gov/d/2024-30983/p-1284.
[69] *Id.* at 962. Available at: https://www.federalregister.gov/d/2024-30983/p-1306.
[70] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1307.

above requires the regulated entity to review and test the policies and procedures at least once every 12 months to satisfy the requirements of these proposals. The creation of these policies and procedures and their continued review have the potential to be both cost and labor-intensive. As such, APhA asks HHS to develop checklists regarding which documents need to be reviewed every 12 months and other educational tools that will aid regulated entities in their efforts to comply with these rules. Further, as discussed earlier, any incentives or funding that HHS can provide to these entities will promote faster adoption and compliance with these proposals.

Section 164.312 – Technical Safeguards (FR 962)

Currently, 45 CFR 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." HHS "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."[71] HHS "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." Regarding 45 CFR 164.312(b)(1) and the encryption and decryption standard, HHS "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."[72] HHS proposes to "add a standard for configuration management at proposed 45 CFR 164.312(c)(1)" that "would require a regulated entity to establish and deploy technical controls for securing relevant electronic information systems and technology assets in its relevant electronic information systems, including workstations, in a consistent manner."[73] Proposed changes to 45 CFR 164.312(d)(1) intend to "improve the effectiveness of audit controls deployed by a regulated entity."[74] Regulated entities, under 45 CFR 164.312(e), "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

[71] *Id.* at 965. Available at: https://www.federalregister.gov/d/2024-30983/p-1372.
[72] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1429.
[73] *Id.* at 971. Available at: https://www.federalregister.gov/d/2024-30983/p-1466.
[74] *Id.* at 973. Available at: https://www.federalregister.gov/d/2024-30983/p-1492.

operational changes, whichever is more frequent, and modify as reasonable and appropriate."[75]

Regarding the authentication standard, under 45 CFR 164.312(f)(1), regulated entities would be required "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."[76] HHS also "propose[s] 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" under the proposed transmission security standard.[77] The proposed vulnerability management "would require a regulated entity to deploy technical controls to identify and address technical vulnerabilities in the regulated entity's relevant electronic information systems."[78] Under 45 CFR 164.312(i)(1) and the data backup and recovery standard, regulated entities would be required "to deploy technical controls to create and maintain exact retrievable copies of ePHI."[79] HHS "also proposes to add a new standard for backup and recovery of relevant electronic information systems at proposed 45 CFR 164.312(j)" by "requir[ing] a regulated entity to deploy technical controls to create and maintain backups of relevant electronic information systems."[80]

APhA generally supports HHS's proposed modifications within this section, as additional guidance and updates to the rules are necessary to account for technological changes since the last update and combat the increase in cybersecurity attacks. APhA notes that many of the requirements outlined in this section will impact the vendors that provide these services to health care entities and providers, including pharmacists and pharmacies. APhA encourages HHS to promote opportunities for these vendors to collaborate with health care providers and entities to ensure that full compliance with these proposed rules and standards can be realized. Additionally, APhA recommends that HHS provide additional insight and guidance related to these rules to small and rural health care entities that may lack the resources and means to effect these changes.

---

[75] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1502.
[76] *Id.* at 977. Available at: https://www.federalregister.gov/d/2024-30983/p-1504.
[77] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1541.
[78] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1562.
[79] *Id.* at 979. Available at: https://www.federalregister.gov/d/2024-30983/p-1585.
[80] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1590.

Section 164.314 – Organizational Requirements (FR 980)

Under 45 CFR 164.314(a)(2), business associate agreements are required to "include provisions compelling a business associate to do all of the following: (1) comply with the requirements of the Security Rule; (2) ensure that any subcontractors that create, receive, maintain, or transmit ePHI on behalf of the business associate agree to comply with the applicable requirements of the Security Rule by also entering into a business associate agreement; and (3) report to the covered entity any security incident of which it becomes aware, including breaches of unsecured PHI as required by the Breach Notification Rule."[81] Further, "45 CFR 164.314(a)(2)(iii) requires that a business associate and its subcontractor enter into a business associate agreement that meets the same requirements as those that apply to a business associate agreement between a covered entity and business associate."[82] Another requirement of business associate agreements is "a provision that requires a business associate to report to the covered entity any known security incident."[83] HHS notes that this notification is important because the security incident could restrict the covered entity's access to the business associate's ePHI or electronic information systems and affect the covered entity's own ePHI or electronic information systems.[84] As such, HHS "proposes to add an implementation specification at proposed 45 CFR 164.314(a)(2)(i)(D) that would require a business associate agreement to include a provision for a business associate to report to the covered entity activation of its contingency plan that would be required under 45 CFR 164.308(a)(13) without unreasonable delay, but no later than 24 hours after activation."[85]

APhA acknowledges the importance the notification of a security incident can have on a covered entity's ability to respond to this emergency or breach. As such, APhA supports the implementation specification that requires a business associate to report to the covered entity when it experiences a security incident and activates its contingency plan within 24 hours of activation.

Section 164.318 – Transition Provisions (FR 986)

"[T]he compliance dates for the initial implementation of the security standards for health plans, health care clearinghouses, and health care providers" were established by

[81] *Id.* at 980. Available at: https://www.federalregister.gov/d/2024-30983/p-1618.
[82] *Id.* at 981. Available at: https://www.federalregister.gov/d/2024-30983/p-1624.
[83] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1625.
[84] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1636.
[85] *Id.* at 982. Available at: https://www.federalregister.gov/d/2024-30983/p-1644.

45 CFR 164.318.[86] HHS "proposes to remove the information in 45 CFR 164.318 and replace the language with provisions for transitioning to the revised Security Rule, should the proposals included in this NPRM be adopted."[87] This proposed rule accounts for a regulated entity's "existing contracts that are not set to terminate or expire until after the compliance date for a final rule modifying the Security Rule" and acknowledges that the "six-month compliance period may not provide enough time to reopen and renegotiate all contracts, in addition to ensuring that all regulated entities are compliant with the revised Security Rule."[88] HHS "proposes to add new transition provisions under 45 CFR 164.318 to allow regulated entities to continue to operate under certain existing business associate agreements or other written arrangements until the earlier of: (1) the date such contract or other arrangement either is renewed on or after the compliance date of the final rule; or (2) a year after the effective date of the final rule."[89] HHS notes that this "additional transition period would be available to regulated entities if both of the following conditions are met: (1) prior to the publication date of the final rule, the covered entity or business associate had an existing business associate agreement or other written arrangement with a business associate or subcontractor, respectively, that complied with the Security Rule prior to the effective date of a final rule revising the Security Rule; and (2) such contract or arrangement would not be renewed or modified between the effective date and the compliance date of the final rule."[90]

APhA appreciates HHS providing an extension to the compliance date for this subsection of the proposed rule and agrees it may be impractical for regulated entities to negotiate all of these new agreements while simultaneously working towards compliance with the other sections of this proposed rule. If adopted, APhA encourages HHS to apply similar extensions to other provisions of the rule to allow time for entities to implement these changes. Extending the compliance dates would be of great benefit, especially to those small and rural health care providers that may not have the resources or finances to make these changes swiftly.

[86] *Id.* at 986. Available at: https://www.federalregister.gov/d/2024-30983/p-1719.
[87] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1721.
[88] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1722.
[89] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1728.
[90] *Id.* Available at: https://www.federalregister.gov/d/2024-30983/p-1728.

New and Emerging Technologies Request for Information (FR 988)

The proposed rule also seeks input regarding privacy and security concerns associated with quantum computing, artificial intelligence (AI), virtual reality (VR), and augmented reality (AR).

APhA appreciates HHS's efforts to learn more about these new and emerging technologies and their potential impacts on the security and privacy of ePHI. Once more information is collected about these technologies, APhA encourages HHS to provide additional guidance regarding how health care entities can ensure compliance with the Security Rule while utilizing them.

Regulatory Impact Analysis (FR 992)

As previously mentioned, APhA is seriously concerned about the significant costs of implementing the proposed rules and standards. This concern peaks when considering the small and rural health care providers already struggling financially to keep their doors open for their patient populations and communities. In addition to the financial costs of implementation, these proposed rules and standards are also labor-intensive, as they will require continued review, testing, and reworking of the initial standards as part of the required review processes. APhA stresses that over 2,200 pharmacies have closed in the United States since 2020.[91] Forcing pharmacies to adopt all these rules and standards quickly and without assistance could result in more pharmacy closures, leaving patients without access to their medications and pharmacist-provided direct care. While APhA sees the value and need to update the Security Rule, APhA asks HHS to find a balance between implementing best practices to ensure that ePHI remains protected and not overburdening health care providers, especially small and rural providers. APhA believes this balance could be found by setting the compliance date beyond the suggested 180 days or providing incentives or finances to entities to help implement these rules and standards.

APhA appreciates the opportunity to respond to HHS's proposed rule and standard changes related to the Security Rule. APhA recommends HHS reconsider the breadth of some of these provisions to avoid overburdening regulated entities with layers of regulations. Further, APhA urges HHS to provide incentives or funding for some of these changes to ensure quicker adoption of these rules and standards so as not to cause

[91] Local Pharmacies on the Brink, New Survey Reveals. National Community Pharmacists Association (Feb. 27, 2024). Available at: https://ncpa.org/newsroom/news-releases/2024/02/27/local-pharmacies-brink-new-survey-reveals.

financial distress for some of the regulated entities. If you have any questions or would like to meet with APhA to discuss our comments, please contact Corey Whetzel, APhA's Senior Manager, Regulatory Affairs, at cwhetzel@aphanet.org.

Sincerely,

Michael Baxter
Vice President, Government Affairs