C. Regulated Entities' Compliance With the Requirements of the Security Rule Is Inconsistent

Despite the proliferation of cybersecurity standards, guidelines, best practices, methodologies, procedures, and processes and the documented increase in unauthorized uses and disclosures of ePHI, many regulated entities have been slow to strengthen their security measures to protect ePHI and their information systems that create, receive, maintain, or transmit it in this new environment.[1] Among the reasons for this are the rapid pace of EHR adoption and digitization of health care, increased connectivity and use of cloud-based infrastructures, limited competition and a stable customer base, limited operating margins, and a failure to invest in cybersecurity infrastructure.[2] For example, regulated entities continue to rely on legacy systems and software that are unsupported by manufacturers, which means that the manufacturers no longer provide security patches or other updates to address security threats and vulnerabilities.[3] In a 2021 survey of health care cybersecurity professionals, 73 percent reported having legacy

[1] Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, p. 2 (explaining that NCVHS conducted an inquiry into whether compliance with the Security Rule had improved since the Department released the results of its 2016-2017 audit of selected provisions of the Security Rule and found that "not much had changed"); "Muddling through cybersecurity: Insights from the U.S. healthcare industry," *supra* note 116, p. 540 ("There is enough evidence to suggest that U.S. healthcare organizations lack a deliberate, organized, and comprehensive cyberresilience strategy.").

[2] *See* Susan Kiser, et al., "Ransomware: Healthcare Industry at Risk," Journal of Business and Accounting, p. 6566 (Fall 2021); Meghan Hufstader Gabriel, "Data Breach Locations, Types, and Associated Characteristics Among US Hospitals," American Journal of Managed Care, p. 78 (Feb. 2018); "Is the HIPAA Security Rule Enough to Protect Electronic Personal Health Information (PHI) in the Cyber Age?" *supra* note 207, p. 20-23.

[3] Chris Hayhurst, "On Guard: Staying Vigilant Against Medical Device Vulnerabilities," Biomedical Instrumentation & Technology, Volume 54, Issue 3, p. 169 (May/June 2020); "Report on Improving Cybersecurity In The Health Care Industry," *supra* note 117, p. 2.

operating systems.[45] This apparent lack of urgency in adopting new, supported operating systems has serious implications for the confidentiality, integrity, and availability of ePHI.

In addition, many regulated entities fail to invest adequate resources in cybersecurity. Far too many regulated entities do not view cybersecurity as a necessary component of their operations that allows them to fulfill their health care missions. Anecdotal evidence suggests that senior management often lacks awareness of cybersecurity, including both threats and methods for protecting against such threats.[6] "A lack of maturity and effectiveness of the [information technology] function is evident when healthcare organizations fail to maintain a current inventory of sensitive and valuable data and where those reside."[7] While maintaining an accurate and thorough inventory of technology assets is not currently an explicit requirement of the Security Rule, it is clearly a fundamental component of conducting a risk analysis and many of the other existing requirements.[8] And yet, based on the Department's experience, many regulated entities are not maintaining such an inventory. At least in part because of senior management's lack of cybersecurity awareness, many fail to invest or fail to invest appropriately in cybersecurity infrastructure.[9] Given the vulnerability of ePHI and the information systems of regulated entities and the potential effects of cyberattacks on patient safety and the delivery of health care, it is important that regulated entities prioritize such investments.[236]

---

[4] "2021 HIMSS Healthcare Cybersecurity Survey," Healthcare Information and Management Systems Society, p. [5] (Jan. 28, 2022),
https://www.himss.org/sites/hde/files/media/file/2022/01/28/2021_himss_cybersecurity_survey.pdf.
[6] "Muddling through cybersecurity: Insights from the U.S. healthcare industry," *supra* note 116, p. 543.
[7] *Id*. at 542.
[8] *See* 68 FR 8334, 8352 (Feb. 20, 2003). In the preamble to the 2003 Security Rule, the Department explained that it had determined that an inventory requirement was unnecessary because it is redundant of other requirements. We assumed that covered entities (and later all regulated entities) would have performed this activity by virtue of having implemented the security measures required under the security management process standard.
[9] "Muddling through cybersecurity: Insights from the U.S. healthcare industry," *supra* note 116, p. 542-543. [236] Eric C. Reese, "Healthcare's cybersecurity stakes reach alarming levels," Health Facilities Management Magazine, Volume 76, Issue 8, p. 22 (Nov. 2022).

The security of ePHI also is at risk because, despite our explanation of the Security Rule's structure in 2003,[10] regulated entities are not fully complying with the standards and implementation specifications. From 2016 to 2017, the Department conducted audits of 166 covered entities and 41 business associates regarding compliance with selected provisions of the HIPAA Rules, including the required implementation specifications for risk analysis[11] and risk management.[12] The Department found that most regulated entities failed to implement the Security Rule requirements for risk analysis and risk management, requirements that are fundamental to protecting the confidentiality, integrity, and availability of ePHI.[240] While most of the audited business associates reported not having experienced any breaches of unsecured PHI, we found that those that had experienced a breach generally engaged in minimal or negligible efforts to address the risk analysis and risk management requirements.[13] According to the report, at that time only 14 percent of covered entities and 17 percent of business associates were "substantially fulfilling their regulatory responsibilities to safeguard ePHI they [held] through risk analysis activities,"[14] while 94 percent of covered entities and 88 percent of business associates "failed to implement appropriate risk management activities sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level."[15] The report specifically noted that the audit results were consistent with the findings of OCR's compliance reviews and complaint investigations.[16]

Recent enforcement actions provide evidence that the results of the 2016-2017 audits were not isolated cases. In 2023, OCR entered into seven resolution agreements with regulated

---

[10] 68 FR 8334, 8343 (Feb. 20, 2003).
[11] 45 CFR 164.308(a)(1)(ii)(A).
[12] 45 CFR 164.308(a)(1)(ii)(B); "2016-2017 HIPAA Audits Industry Report," *supra* note 121, p. 4. [240] "2016-2017 HIPAA Audits Industry Report," *supra* note 121, p. 4.
[13] *Id.* at 11.
[14] *Id.* at 27.
[15] *Id.* at 30.
[16] *Id.* at 27 and 30.

entities after investigations indicated that they had potentially violated the Security Rule, constituting almost half of the total resolution agreements OCR entered into that year.[17] In each case, OCR's investigation found evidence of multiple potential violations. For example, in one case, a regulated entity did not detect an intrusion into its network until 20 months later when its files were encrypted with ransomware.[18] OCR's investigation found evidence of potential failures of the regulated entity to conduct a risk analysis or to sufficiently monitor information system activity. OCR also found evidence that the regulated entity may not have had policies and procedures in place to implement the requirements of the Security Rule to protect the confidentiality, integrity, and availability of ePHI.[19]

As another example, an OCR investigation of a large health care system found indications of multiple potential violations of the Security Rule, including failures by the regulated entity to conduct a risk analysis, monitor and safeguard its electronic information systems, and implement policies and procedures to record and examine activity in its electronic information systems containing ePHI.[20] The regulated entity was not only unable to prevent the cyberattack, but it was unaware the attack had occurred until two years later. This is despite the long-standing requirements of the Security Rule and the obligations imposed on regulated entities for risk analysis and risk management.

---

[17] *See* "OCR News Releases & Bulletins," Office for Civil Rights, U.S. Department of Health and Human Services, https://www.hhs.gov/ocr/newsroom/index.html.

[18] *See* Resolution Agreement, "Doctors' Management Services, Inc.," Office for Civil Rights, U.S. Department of Health and Human Services (Oct. 31, 2023), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/dms-ra-cap/index.html; Press Release, "HHS' Office for Civil Rights Settles Ransomware Cyber-Attack Investigation," Office for Civil Rights, U.S. Department of Health and Human Services (Oct. 31, 2023), https://www.hhs.gov/about/news/2023/10/31/hhs-office-civil-rights-settles-ransomware-cyber-attackinvestigation.html; *see also* "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information," *supra* note 10.

[19] "HHS' Office for Civil Rights Settles Ransomware Cyber-Attack Investigation," *supra* note 246.

[20] *See* Resolution Agreement, "Montefiore Medical Center," Office for Civil Rights, U.S. Department of Health and Human Services (Nov. 17, 2023), https://www.hhs.gov/hipaa/for-professionals/complianceenforcement/agreements/montiefore/index.html; "HHS' Office for Civil Rights Settles Malicious Insider Cybersecurity Investigation for $4.75 Million," *supra* note 223.

Despite the long-standing nature of the Security Rule and the proliferation of guidance documents from NIST, the Department, CISA, FTC, and others, regulated entities continue to fail to implement reasonable and appropriate security measures as required by the Security Rule.[21] For example, the Security Rule and NIST guidance have addressed encryption for data in transit and at rest for many years.[22] And yet, in the 2021 survey of health care cybersecurity professionals, only half of the respondents reported having implemented encryption for data in transit across the enterprise.[23] Similarly, according to its CEO, a large covered entity failed to deploy multi-factor authentication (MFA) throughout its enterprise and experienced a significant breach.[24] If this is accurate, it would run counter to long-standing provisions in both the Security Rule and NIST guidance; the Security Rule has required the implementation of appropriate access controls since 2003 and NIST recommends similar controls.[253]

As another example, based on OCR's investigation experience, some regulated entities are not developing and implementing compliant response plans for security incidents, including those that are breaches of unsecured ePHI under the Breach Notification Rule. Section 164.308(a)(6)(i) establishes the standard that requires regulated entities to implement policies and procedures to address security incidents, while 45 CFR 164.308(a)(6)(ii) includes the implementation specifications for that standard. This requirement, included in the 2003 Final Rule, aligns with the NIST Cybersecurity Framework version 2.0 requirement for incident management.[254] Similarly, NIST Cybersecurity Framework version 1.1 recommended the execution and maintenance of response processes and procedures to ensure response to detected

---

[21] "Muddling through cybersecurity: Insights from the U.S. healthcare industry," *supra* note 116, p. 541; "Start with Security: A Guide for Business," *supra* note 17.

[22] *See* 45 CFR 164.312(a)(1) and (e)(1); PR.DS-1 and 2, "Framework for Improving Critical Infrastructure Cybersecurity," Cybersecurity Framework (CSF) Version 1.1, National Institute of Standards and Technology, U.S. Department of Commerce (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf; PR.DS-01 and 02, "The NIST Cybersecurity Framework (CSF) 2.0," *supra* note 15.

[23] "2021 HIMSS Healthcare Cybersecurity Survey," *supra* note 231, p. 23.

[24] *See* "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next," *supra* note 214 (According to CEO Andrew Witty, intruders used compromised credentials to remotely access an

cybersecurity incidents.[255] And yet, when OCR investigates the circumstances surrounding breach reports, OCR continues to find evidence that regulated entities have not implemented policies and procedures to detect and respond to security incidents, leading to significant time lapses between a "successful" security incident[256] and discovery of, and response to, the security incident.[257] Thus, based on the OCR's experience investigating and enforcing the Security Rule, the Department believes that many regulated entities would benefit from additional instruction in regulatory text regarding their compliance obligations to determine how to select security measures that are reasonable and appropriate for their circumstances.

We are also concerned that recent caselaw has not accurately set forth the steps regulated entities must take to adequately protect the confidentiality, integrity, and availability of ePHI, as required by the statute. Specifically, in the *University of Texas M.D. Anderson Cancer Center* v. *HHS* ("*M.D. Anderson*"), the U.S. Court of Appeals for the Fifth Circuit held, among other things, that the Security Rule does not say anything about how effective a mechanism for encryption must be, nor does it require that an encryption mechanism provide "bulletproof protection" of all systems containing ePHI.[25] Thus, under the court's interpretation, a regulated entity can meet its obligations under the Security Rule concerning encryption and decryption of ePHI by implementing a mechanism to do so, without regard for the effectiveness of the

application used to enable remote access to desktops, which did not have MFA.). The Department's investigation into the Change Healthcare breach is ongoing, and no conclusion has been reached with respect to its cause or whether Change Healthcare was in violation of the Security Rule.

[253] 45 CFR 164.308(a)(4)(ii)(B) and 164.312(a)(1); "The NIST Cybersecurity Framework (CSF) 2.0," *supra* note 15; "Framework for Improving Critical Infrastructure Cybersecurity," *supra* note 250.

[254] RS.MA, "The NIST Cybersecurity Framework (CSF) 2.0," *supra* note 15.

[255] PR.IP-9, "Framework for Improving Critical Infrastructure Cybersecurity," *supra* note 250.

[256] 45 CFR 164.304 (definition of "Security incident"). The definition of security incident includes both attempted and successful incidents. A successful incident is one in which a threat actor is able to, without authorization, access, use, disclose, modify, or destroy information or interfere with system operations in an information system. [257] *See, e.g.*, "Montefiore Medical Center," *supra* note 248.

[25] *University of Texas M.D. Anderson Cancer Center* v. *U.S. Department of Health and Human Services*, 985 F.3d 472, 478 (5th Cir. 2021).

implementation.[26] Additionally, the court noted that the requirement for "a mechanism" does not "prohibit a [regulated] entity from creating 'a mechanism' by directing employees to sign an [agreement] that requires the encryption of portable devices."[27] While the Department disagrees with the court's interpretation that merely requiring employees to sign an agreement to encrypt portable devices is sufficient to comply with its Security Rule obligations to implement a mechanism to encrypt and decrypt ePHI, the Department believes that additional clarity is warranted to ensure that regulated entities understand their obligation to have encryption mechanisms in place and deployed throughout the regulated entity's enterprise to ensure the confidentiality, integrity, and availability of ePHI.

Several technical safeguards currently require regulated entities to implement a "mechanism" as part of complying with the associated standard. Given that written policies and procedures alone are insufficient to protect ePHI, and the misinterpretation of what it means to implement a mechanism also could lead to inadequate protection of ePHI, the Department believes that the Security Rule must be revised, consistent with its statutory mandate, as discussed in greater detail above.

[26] *Id.*
[27] *Id.*

D. It Is Reasonable and Appropriate to Strengthen the Security Rule To Address the Changes in the Health Care Environment and Clarify the Compliance Obligations of Regulated Entities

1. Congress and the Department Anticipated That Security Standards Safeguards Would Evolve To Address Changes in the Health Care Environment

By requiring that regulated entities maintain reasonable and appropriate safeguards to protect against reasonably anticipated threats or hazards or unauthorized uses or disclosures of ePHI, Congress clearly anticipated that the administrative, physical, and technical safeguards implemented to protect the security of ePHI would need to change in response to changes in the environment in which health care is provided.[28] As the health care environment and the operations of regulated entities evolve, so must the protections for ePHI and the information systems used to create, receive, maintain, or transmit it. For example, regulated entities must be expected to adopt safeguards that address new risks to the security of ePHI, such as those posed by maintaining ePHI in the cloud; the connection of medical devices and other technology to networks; and the connection of information systems used to create, receive, maintain, or transmit ePHI to the same networks as those do not perform such activities. After all, it is reasonable to anticipate that there will be new threats or hazards to ePHI or efforts by unauthorized persons to use or disclose such ePHI in an increasingly connected environment.

[28] Sec. 1173(d)(2)(B) of Pub. L. 104–191, 110 Stat. 2026 (Aug. 21, 1996) (codified at 42 U.S.C. 1320d–2). [262] 68 FR 8334, 8336 (Feb. 20, 2003).

By design, the Security Rule sets a national floor for the security measures that regulated entities are required to implement to protect the confidentiality, integrity, and availability of ePHI. In 2003, the Department opted to frame the standards in terms that were as generic as possible and in a manner that enabled the standards to be met through various approaches or technologies to ensure that regulated entities had the flexibility to determine how best to protect the confidentiality, integrity, and availability of ePHI based on their specific circumstances.[262] When we extended the Security Rule in 2013 to directly apply to business associates in accordance with the HITECH Act,[29] the Department acknowledged that some business associates might not have engaged in the formal administrative safeguards required by the Security Rule, and we made it clear that business associates would be expected to do so going forward.[30] Despite the changes in the health care environment between 2003 and 2013, the Department made minimal changes to the Security Rule at that time because we believed that the compliance obligations of regulated entities were clear and well-understood. In fact, when a commenter recommended that the Department remove the "addressable" designation from the Security Rule because it leads to ambiguity in the rule's application, we declined to do so at that time because we were concerned that it would reduce the rule's scalability and flexibility.[31] However, as we noted in 2003, the rule's flexibility of approach is primarily provided for in paragraph (b)(2) of 45 CFR 164.306 and in the standards themselves.[32] The addressability feature merely provided an added level of flexibility[267] in a way that the Department now believes is inadequate to ensure that regulated entities implement reasonable and appropriate security safeguards.

[29] 42 U.S.C. 17931(a); 78 FR 5566 (Jan. 25, 2013).
[30] 78 FR 5566 (Jan. 25, 2013).
[31] *Id*. at 5591.
[32] *See* 68 FR 8334, 8341 (Feb. 20, 2003). [267]
Id. at 8344.

Changes to the health care environment and the operations of regulated entities have increased the importance of implementing strong security measures to protect ePHI and the information systems that create, receive, maintain, or transmit it. While we recognize the burdens posed by such implementation on regulated entities, there is also a clearly documented increase in the number of breaches of unsecured PHI and instances of cybercriminals accessing ePHI without authorization at regulated entities. The changes to the health care environment, including the increase in breaches and cyberattacks, and operations of regulated entities have made it increasingly likely that unauthorized persons will seek to obtain ePHI and disrupt the U.S. health care system. Additionally, the clearly documented failure of regulated entities to fully implement the policies and procedures required by the Security Rule and apply the required security measures throughout their operations has caused the Department to question whether the existing Security Rule should be revised to clarify and strengthen the obligations of regulated entities and revisit our decision from 2013.[33] In many cases involving a breach of ePHI that OCR has investigated, a breach may not have occurred, or would have been less widespread and disruptive, had the regulated entities fully implemented the provisions of the Security Rule.[34]

2. NCVHS Believes That the Security Standards Evolve To Address Changes in the Health Care Environment

The Department is not alone in believing that the Security Rule should be strengthened to address concerns about whether -regulated entities are sufficiently protecting the confidentiality, integrity, and availability of ePHI. An inquiry conducted by NCVHS between July 2021 and

[33] *See* "2016-2017 HIPAA Audits Industry Report," *supra* note 121, p. 4 ("[M]ost covered entities failed to meet the requirements for other selected provisions in the audit, such as adequately safeguarding protected health information (PHI) [...] OCR also found that most covered entities and business associates failed to implement the HIPAA Security Rule requirements for risk analysis and risk management."); "Enforcement Highlights," Office for Civil Rights, U.S. Department of Health and Human Services, https://www.hhs.gov/hipaa/forprofessionals/compliance-enforcement/data/enforcement-highlights/index.html.
[34] *See, e.g.*, "Montefiore Medical Center," *supra* note 248; "Doctors' Management Services, Inc.," *supra* note 246.
[270] Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, p. 2 (detailing the inquiry undertaken by NCVHS into the scope and breadth of security risks and how to best address those challenges).

September 2023 reached the same conclusion.[270] During this inquiry, NCVHS listened to the testimony of cybersecurity experts and Department officials. The experts and Department officials "consistently voiced their concerns about the major increase in incidents and, in particular, the widespread lack of robust risk analysis on the part of covered entities and business associates that would lead to prior planning for, and mitigation of, a range of cybersecurity threats."[35] In response to this inquiry and consistent with their statutory mandate,[36] NCVHS transmitted two letters to the Secretary with recommendations for improving cybersecurity practices in the health care industry, including recommendations for modifying the Security Rule.[37] As part of the explanation for its concerns, NCVHS cited a 2021 survey of acute and ambulatory care organizations that found only 32 percent of those organizations had a comprehensive security program, while only 26 percent of the long-term and post-acute care facilities met the minimum security requirements.[38] Specifically, NCVHS made the following recommendations for improvements to the Security Rule:

- Eliminate from the addressable implementation specifications the choice not to implement a specification or alternative, and instead require regulated entities to implement the specification or adopt a documented reasonable alternative.[275]
- Include specific minimum cybersecurity hygiene requirements that are reflective of modern industry best practices, including designation of a qualified information security official, elimination of default passwords, adoption of MFA, institution of offline

---

[35] *Id.*

[36] *See* 42 U.S.C. 1320d-1(f).

[37] *See* Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123; Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123.

[38] *See* Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123, p. 4 (citing a survey performed by a College of Healthcare Information Management Executives (CHIME) as explained at Jill McKeon, "32% of Healthcare Organizations Have a Comprehensive Security Program," Health IT Security (Nov. 22, 2021), https://healthitsecurity.com/news/32-of-healthcare-organizations-have-a-comprehensive-securityprogram). [275] *See* Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123, p. 4; *see also* Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 1.

backups, installation of critical patches within a reasonable time, and transparency of impact and vulnerability disclosures.[39]

- Require that regulated entities implement a security program and that they implement standard minimum security controls.[40]
- Require that regulated entities adopt a risk-based approach in their security program.[41]
- Require that regulated entities perform a risk analysis in a manner that conforms with guidance from NIST and CISA.[42]
- Define compensating controls more specifically and provide a wider range of examples that apply to a greater variety of types of entities.[43]
- Reinforce the need for regulated entities to account for AI systems and data within their risk analysis for all and any new technology.[44]
- Establish a consistent floor for cyber incident reporting and harmonize such requirements with incident reporting provisions applicable to health care critical infrastructure actors and health care Federal contractors.[45]

The Department, in drafting this NPRM, relied on the recommendations of NCVHS, OCR's enforcement experience, news reports, and our assessment of the environment. Consistent with NCVHS' recommendation to revisit the Security Rule's classification of some implementation specifications as "addressable," the Department also believes that it is appropriate to revisit our decision regarding the amount of flexibility regulated entities have in

[39] *See* Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123, p. 5-10; *see also* Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 2.
[40] Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123, Appendix p. 1-4.
[41] *Id.* at Appendix p. 4-5.
[42] *Id.* at Appendix p. 4-6.
[43] *Id.* at Appendix p. 6-7.
[44] *Id.* at Appendix p. 7-8.
[45] *Id.* at 9-10.

determining reasonable and appropriate safeguards, as described above. Based on OCR's experience in investigations and audits, we believe that regulated entities would benefit from greater specificity in the Security Rule. The Department has provided extensive guidance on questions to consider when adopting and implementing security measures and ways to comply with the Security Rule,[46] as directed by the HITECH Act. And yet, despite this proliferation of guidance, regulated entities continue not to comply. For example, despite the explanation in 45 CFR 164.306(d) about addressable implementation specifications and the notable changes in the environment in which health care is provided, we are concerned that some regulated entities proceed as if compliance with an addressable implementation specification is optional—and that where there is an addressable implementation specification, that compliance with the relevant standard is also optional. That interpretation is incorrect and weakens the cybersecurity posture of regulated entities. We believe that compliance with the implementation specifications currently designated as addressable is not—and should not be—optional, particularly in light of the shift to an interconnected and cloud-based environment and a significant increase in the number of breaches of unsecured PHI from both internal and external actors, regardless of the regulated entity's specific circumstances. Thus, we believe that it is necessary to strengthen the Security Rule to reflect the changes in the health care environment and the evolution of technology and to underscore that compliance with all of our proposals, if finalized, is required.

3. A Strengthened Security Rule Would Continue To Be Flexible and Scalable While Providing Regulated Entities With Greater Clarity The Security Rule's fundamental flexibility and scalability generally would

[46] The Department has issued, among other things, a video presentation on trends in real world cyberattacks, a cybersecurity checklist and infographic, guidance on ransomware, a crosswalk with the NIST CSF, and an ongoing series of newsletters on various topics pertaining to cybersecurity. *See* "Cyber Security Guidance Material," Office for Civil Rights, U.S. Department of Health and Human Services, https://www.hhs.gov/hipaa/forprofessionals/security/guidance/cybersecurity/index.html.

remain should the proposals in this NPRM be adopted. However, we are proposing to reduce that flexibility to better strengthen protections and address the changed nature of the environment in which health care is provided. The Department is also proposing in this NPRM to strengthen the Security Rule by providing greater clarity regarding the nature of its flexibility and scalability and the Department's expectations, as requested by regulated entities and other stakeholders. In fact, in response to a request for information published in 2022,[47] several commenters urged the Department to propose regulations that establish a single set of clear standards for regulated entities, raise the floor for security requirements and expectations, and encourage regulated entities to safeguard ePHI while maintaining flexibility and scalability. Commenters also encouraged the Department to rely on commonly available, non-proprietary frameworks that allow regulated entities to adopt critical security measures. We believe that our proposals are consistent with those recommendations.

Under the proposal, regulated entities would retain the ability to determine the security measures that are reasonable and appropriate to fulfill the required standards and implementation specifications, taking into consideration the factors listed at proposed 45 CFR 164.306(b)(2). In fact, the NPRM, if adopted as proposed, would add to the rule's flexibility and scalability by adding a new factor for regulated entities to consider when determining the reasonable and appropriate security measures.[48]

[47] *See* 87 FR 19833 (Apr. 6, 2022).
[48] *See* proposed 45 CFR 164.306(b)(2)(v).

Additionally, if modifications are adopted as proposed, the Security Rule would remain flexible and scalable by retaining broad standards with which regulated entities could comply in a variety of ways. In 2003, the 13 implementation specifications that the Security Rule requires were considered so basic that no covered entity could effectively protect ePHI without implementing them.[49] While the Department agrees that these implementation specifications remain essential, we no longer believe that they are sufficient to address the risks to ePHI today. Rather, regulated entities must do more to ensure the confidentiality, integrity, and availability of ePHI today because of the changes in the environment in which health care is provided, how ePHI is maintained, the level of connectivity between information systems, and the technological sophistication of bad actors.

We acknowledged in 2003 and again acknowledge here that "there is no such thing as a totally secure system that carries no risks to security."[50] We posited at that time that Congress intended to set an "exceptionally high goal for the security of [ePHI]," while also recognizing that securing ePHI did not require that covered entities do so without regard for the cost.[51] However, we also made clear that a covered entity is required to implement adequate security measures and that cost was but one factor for a covered entity to consider when determining what constituted appropriate security measures.[52] As we noted, "Cost is not meant to free covered entities from this responsibility."[290] In the 2013 Omnibus Rule, we further explained that "[regulated entities] have the flexibility to choose security measures appropriate for their size, resources, and the nature of the security risks they face, enabling them to reasonably implement any given Security Rule standard. […] Thus, the costs of implementing for […] business

---

[49] 68 FR 8334, 8336 (Feb. 20, 2003).
[50] *Id*. at 8346.
[51] *Id.* At that time, the Security Rule applied directly only to covered entities. As discussed above, Congress later extended the application of the Security Rule directly to business associates.
[52] 68 FR 8334, 8343 (Feb. 20, 2003). [290]
Id.

associates will be proportional to their size and resources."[53] We continue to believe that this is the case. Additionally, as discussed above, there is a significant cost associated with breaches and unauthorized access—financial, reputational (for both the individual and the regulated entity), and more. Thus, we believe that the standards and implementation specifications that we propose in this NPRM are the minimum that regulated entities should be doing to protect the security of ePHI and lower the costs associated with breaches and other incidents.

4. Small and Rural Health Care Providers Must Implement Strong Security Measures To Provide Efficient and Effective Health Care

The statute requires that we consider the "needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary)."[54] We recognize that small and rural health care providers may have needs and capabilities that differ from those of other regulated entities. For example, small health care providers and rural health care providers are often located at a greater distance from other health care providers.[55] It may be more challenging for them to attract and retain clinicians and administrative support staff.[56] They also face difficulty attracting and retaining security experts and must make difficult decisions regarding investments in competing priorities.[295] Often, preparation for security incidents or other occurrences that adversely affect the confidentiality, integrity, or availability of ePHI is

[53] 78 FR 5566, 5589 (Jan. 25, 2013).
[54] 42 U.S.C. 1320d–2(d)(1)(A)(v).
[55] *See* "Why Health Care is Harder to Access in Rural America," U.S. Government Accountability Office (May 16, 2023) (When local hospitals close in rural areas, residents have to travel more than 20 miles further to receive common health care and 40 miles further to receive less common health care, such as substance use disorder treatment. Such rural areas generally have fewer health care providers overall.), https://www.gao.gov/blog/whyhealth-care-harder-access-rural-america.
[56] *See* "A National Staffing Emergency in Rural Health Care," American Hospital Association (Dec. 19, 2023), https://www.aha.org/advancing-health-podcast/2023-12-20-national-staffing-emergency-rural-health-care. [295] *See* Debi Primeau, "How Small Organizations Handle HIPAA Compliance," Journal of the American Health Information Management Association, Volume 88, Issue 4, p. 18-21, 19 (Apr. 2017); Kat Jercich, "Rural hospitals are more vulnerable to cyberattacks – here's how they can protect themselves," Healthcare IT News (Sept. 8, 2021); *see also* Tami Lichtenberg, "Recovering from a Cybersecurity Attack and Protecting the Future in Small, Rural Health Organizations" (Oct. 4, 2023), https://www.ruralhealthinfo.org/rural-monitor/cybersecurity-attacks.

neglected in favor of other priorities, putting small and rural health care providers at greater risk for such an occurrence.[57]

We continue to believe that it is just as important for small and rural health care providers to implement strong security measures as it is for larger health care providers and other categories of regulated entities. According to experts, "Cybercriminals go after small businesses, especially those in the healthcare industry, because they are easy targets."[58] In 2017, 93 percent of small rural and critical access hospitals and 86 percent of physician offices relied on health IT to inform their clinical practice.[298] And yet, small health care providers are less likely than a larger organization to even have a designated security or compliance officer.[59] Smaller practices and rural and community facilities also may be more likely to rely on older technologies that are no longer supported by security patches and updates, including medical devices such as insulin pumps and pacemakers in which inaccuracies or errors could affect patient safety.[60] Thus, small health care providers "are at the greatest risk of a breach. [...] Smaller, rural practice settings are especially high-risk target areas for a breach."[61] According to an expert who speaks to and works with health care providers on IT services and cybersecurity, small health care providers are "more susceptible because they do not have a lot of the tools and security measures necessary to protect themselves."[62] For example, a critical access hospital in Colorado recovered from a cyberattack in 2019, but it required "an incredible amount of staff time, many months of

---

[57] *See* "How Small Organizations Handle HIPAA Compliance," *supra* note 295, p. 19; "Rural hospitals are more vulnerable to cyberattacks – here's how they can protect themselves," *supra* note 295.
[58] "Too Small to Be Attacked by Cybercriminals? Not So Fast," Same-Day Surgery, Volume 43, Issue 7 (July 2019), https://www.reliasmedia.com/articles/144561-too-small-to-be-attacked-by-cybercriminals-not-so-fast. [298] "Percent of Hospitals, By Type, that Possess Certified Health IT," Health IT Quick-Stat #52 (Sept. 2018), https://www.healthit.gov/data/quickstats/percent-hospitals-type-possess-certified-health-it; "Office-based Physician Electronic Health Record Adoption," Health IT Quick-Stat #50, https://www.healthit.gov/data/quickstats/officebased-physician-electronic-health-record-adoption.
[59] "How Small Organizations Handle HIPAA Compliance," *supra* note 295, p. 19.
[60] *See id*.
[61] *Id.*; *see also* "Recovering from a Cybersecurity Attack and Protecting the Future in Small, Rural Health Organizations," *supra* note 295.
[62] "Too Small to Be Attacked by Cybercriminals? Not So Fast," *supra* note 297.

recovery efforts, and an enormous financial outlay to restore systems and prevent another attack."[63] In fact, the hospital estimates that "it took a full year of a staff person's time to complete the recovery and protect the organization for the future."[64] These costs do not include the multiple ransoms paid to the attackers after the first set of keys did not unlock all of the data.[305]

Patients and communities have a critical need for health care providers, including rural hospitals and other rural health care providers, to be resilient and remain operational, which depends in part on the cybersecurity of their electronic information systems. For rural health care providers, especially hospitals, a breach can significantly affect an entire community.[65] Rural health care providers often are separated by significant distances, which can have real consequences for someone experiencing a medical emergency.[66] A recent study comparing hospital characteristics and operations of rural and urban hospitals that experienced ransomware attacks between 2016 and 2021 found that rural hospitals experienced large declines in inpatient admissions and Medicare revenue, similar to those experienced by urban hospitals.[67] The study also found that the decline in volume and revenue of hospital outpatient and emergency room visits was more pronounced among rural facilities.[309] In fact, in June 2023, a hospital in rural Illinois announced that it would close, in part because a 2021 cyberattack prevented it from

---

[63] "Recovering from a Cybersecurity Attack and Protecting the Future in Small, Rural Health Organizations," *supra* note 295.

[64] *Id.* [305]

Id.

[65] *See*, *e.g.*, "Fact Sheet: Biden-Harris Administration Bolsters Protections for Americans' Access to Healthcare Through Strengthening Cybersecurity," The White House (June 10, 2024), https://www.whitehouse.gov/briefingroom/statements-releases/2024/06/10/fact-sheet-biden-harris-administration-bolsters-protections-for-americansaccess-to-healthcare-through-strengthening-cybersecurity/; "How Do Ransomware Attacks Impact Rural Hospitals?," National Institute for Health Care Management Foundation, p. 1 (2024), https://nihcm.org/assets/articles/FINAL-NIHCM-RI-Hannah-Neprash_2024-08-01-132728_ushq.pdf.

[66] "How Do Ransomware Attacks Impact Rural Hospitals?" *supra* note 306, p. 2.

[67] *Id.* [309]

Id.

submitting claims to health plans for months.[68] According to a local elected official, the hospital's closure would require some residents to travel approximately 30 minutes for the nearest emergency room and obstetrics services.[69] Thus, implementing security measures to maintain facility operations is critical to minimize or avoid disruptions to patient care and patient safety activities in such facilities. Consistent with these examples, the Department believes that small and rural health care providers are also viewed as potential targets by cybercriminals, and such providers need to implement strong cybersecurity measures to secure the ePHI in their possession. In fact, in June 2024, the Administration announced a collaboration with the private sector to provide additional cybersecurity resources for rural health care providers in recognition of the importance of protecting the security of ePHI created, received, maintained, or transmitted by such entities.[70] We believe this collaboration will provide small and rural health care providers with additional support, particularly when coupled with other resources described in greater detail below.[71] Thus, we believe that small and rural health care providers have both the need to comply with the proposals in this NPRM and the capability of doing so. Additionally, we believe that the NPRM would continue to provide all regulated entities, including small and rural health care providers, the ability to take into account their circumstances when determining which security measures are reasonable and appropriate.[72]

---

[68] Kevin Collier, "An Illinois hospital is the first health care facility to link its closing to a ransomware attack," NBC News (June 12, 2023), https://www.nbcnews.com/tech/security/illinois-hospital-links-closure-ransomwareattack-rcna85983.

[69] *Id.*

[70] "Fact Sheet: Biden-Harris Administration Bolsters Protections for Americans' Access to Healthcare Through Strengthening Cybersecurity," *supra* note 306.

[71] *See, e.g.*, "Free Cybersecurity Services and Tools," Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security, https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-andtools; "Cyber Hygiene Services," Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland
Security, https://www.cisa.gov/cyber-hygiene-services; "Cybersecurity Resources for High-Risk Communities," Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security, https://www.cisa.gov/audiences/high-risk-communities/cybersecurity-resources-high-risk-communities.

[72] *See, e.g.*, 45 CFR 164.306.

5. A Strengthened Security Rule Is Critical to an Efficient and Effective Health Care System

While the Security Rule generally continues to accomplish a primary goal of HIPAA,[73] the Department believes that it is essential to propose modifications to strengthen its protections for the confidentiality, integrity, and availability of ePHI to address the changing health care environment. We also believe it is important to clarify the obligations of regulated entities and emphasize the importance of protecting the confidentiality, integrity, and availability of ePHI. We believe that the proposed revisions would require regulated entities to consider and potentially modify their safeguards more regularly, which would better enable them to quickly respond to changes in the environment and be consistent with cybersecurity best practices. While we do not expect that compliance with the Security Rule will prevent all breaches or interruptions in the confidentiality, integrity, or availability of ePHI, we believe that it will prevent many and enable regulated entities to identify, mitigate, and remediate the damage more quickly if there is a breach or other security incident, thereby reducing harm to individuals and the overall costs of such occurrences to regulated entities and to the U.S. health care system. As such, the proposed modifications would support a primary goal of HIPAA's Administrative Simplification provisions: improving the efficiency and effectiveness of the U.S. health care system by encouraging the development of health information systems through the establishment of uniform standards and requirements for electronic transmission of ePHI, including those for security.[74]

E. The Secretary Must Develop Standards for the Security of ePHI Because None Have Been Developed by an ANSI-Accredited Standard Setting Organization HIPAA requires the Secretary to adopt standards that have been developed, adopted, or modified by a standard

[73] *See* sec. 261 of Pub. L. 104–191, 110 Stat. 2021 (Aug. 21, 1996), as amended by sec. 1104(a) of Pub. L. 111-148, 124 Stat. 146 (Mar. 23, 2010) (codified at 42 U.S.C. 1320d note).
[74] *Id*.

setting organization accredited by ANSI, except in certain circumstances.[75] For example, HIPAA permits the Secretary to develop standards where no relevant standards have been developed, adopted, or modified by an ANSI-accredited standard setting organization. In developing, adopting, or modifying a standard, the Secretary is required to consult with standard setting organizations, NCVHS, and with the appropriate Federal and State agencies.[318]

The statutory definition of the term "standard" applies only to standards for electronic transactions and data elements for such transactions that are appropriate for: (1) the financial and administrative transactions described in the statute; and (2) other financial and administrative transactions consistent with the goals of improving the operation of the health care system and reducing administrative costs, as determined appropriate by the Secretary.[76] Under HIPAA, security is not considered a financial or administrative transaction, or a data element of such transaction.[77] In the "Health Insurance Reform: Standards for Electronic Transactions" final rule in 2000, we explicitly adopted a broader definition of "standard" because we recognized that the statutory definition only applied to standards for financial and administrative transactions, despite the statute's requirement that the Secretary adopt standards addressing other matters, including privacy and security.[78] At that time, we explained that we adopted a broader definition of standard to accommodate the varying functions of the specific standards proposed in other HIPAA regulations.[79] For the same reason, we believe that it is appropriate to continue to rely on the regulatory definition of standard.[80]

---

[75] 42 U.S.C. 1320d-1(c)(1) and (2). [318]
42 U.S.C. 1320d–1(c)(2)(B).
[76] *See* 42 U.S.C. 1320d(7) (definition of "Standard").
[77] *See* 42 U.S.C. 1320d–2(a)(1).
[78] 65 FR 50312, 50320 (Aug. 17, 2000); *see also* 42 U.S.C. 1320d–2(b), (c), and (d); sec. 264(c) of HIPAA.
[79] 65 FR 50312, 50320 (Aug. 17, 2000).
[80] 45 CFR 160.103 (definition of "Standard").

As discussed above, in both 1998 and 2003, the Department determined that no comprehensive, scalable, and technology-neutral set of standards exists, and accordingly, we proposed and adopted a new standard.[81] In 2013, we made only minor modifications to the standards when we complied with explicit directions from Congress to apply the requirements of the Security Rule to business associates, so we did not need to consider whether an ANSIaccredited standard setting organization had adopted a comprehensive set of standards on the security for ePHI that was flexible, scalable, and technology-neutral.[325]

However, because we believe it is appropriate for us to consider modifying the Security Rule at this time for the reasons discussed above, we must again consider whether an ANSIaccredited standards setting organization has developed, adopted, or modified a standard relating to the security of ePHI. The Department continues to believe that any standard must be comprehensive, rather than piecemeal, as recommended by the ANSI Healthcare Informatics Standards Board.[82] We also continue to agree with the recommendation that the standards should be technology-neutral because security technology continues to evolve to keep pace with the evolution of technology more broadly. Additionally, the Security Rule must remain flexible and scalable to allow for consideration of the wide variety of regulated entities, enabling such entities to determine the reasonable and appropriate security measures for their circumstances by taking into account the factors specified by HIPAA.[83]

We are not aware of any standard setting organizations that are accredited by ANSI that have issued standards for the security of ePHI, let alone standards that are sufficiently comprehensive, flexible, scalable, and technology-neutral to enable regulated entities to take into account the HIPAA factors. For example, NIST has issued numerous publications addressing

---

[81] 63 FR 43242, 43249 (Aug. 12, 1998); 68 FR 8334, 8341 (Feb. 20, 2003). [325]
78 FR 5566, 5589-91, 5693-95 (Jan. 25, 2013).
[82] 63 FR 43249 (Aug. 12, 1998); 68 FR 8341 (Feb. 20, 2003).
[83] 42 U.S.C. 1320d–2(d)(1)(A).

health care cybersecurity that are considered by NIST to be guidance, rather than standards. In fact, NIST is ANSI-accredited for only one standard.[84] And with the exception of publications that analyze the Security Rule, NIST's guidance does not specifically address the security of ePHI. CISA has issued cross-sector CPGs, but it is not ANSI-accredited. There may be other organizations that have set standards for the transmission of particular information, such as the secure transmission of images, but adopting such individual standards would not meet the Department's criteria. In this case, adoption of such standard would be far too granular and require the Department to revise the Security Rule at the same interval as the particular standard, which may be irregular. Additionally, given that the Department is limited to modifying each standard or implementation specification no more frequently than once every 12 months, this approach would be inefficient and could lead to a requirement that the Department update the Security Rule more than once a year, depending on when such individual standards or implementation specifications are revised. Even modifying the standards annually would require a significant investment of Department resources, not to mention the investment required of regulated entities to comply with an ever-changing set of requirements.

Additionally, in 2021, Congress amended the HITECH Act to require the Secretary to consider whether a regulated entity has adequately demonstrated that it had in place recognized security practices for a certain period of time.[85] Congress defined "recognized security practices" to include certain NIST publications; the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015; "and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities."[330] However, the HITECH Act amendment did not require the Secretary to accept a

[84] "ANSI/NIST-ITL Standard," National Institute of Standards and Technology, U.S. Department of Commerce (Feb. 3, 2023), https://www.nist.gov/programs-projects/ansinist-itl-standard.
[85] *See* section 13412(a) of the HITECH Act, as amended by section 1 of Pub. L. 116-321, 134 Stat. 5072 (Jan. 5, 2021) (codified at 42 U.S.C. 17941(a)(1)). [330] *Id.*

regulated entity's implementation of recognized security practices as an alternative to compliance with the Security Rule, nor did it provide that such implementation was sufficient to meet the security objectives of HIPAA or the HITECH Act. Accordingly, it is appropriate for the Department to develop and adopt its own standards to meet the statutory objective of ensuring the security of ePHI. The standards and implementation specifications proposed herein take into consideration not only those promulgated by NIST, but also guidelines, best practices, methodologies, processes, and procedures published by CISA, the HHS 405(d) program, CMS, State governments, and others. The proposals also enable regulated entities to adopt security measures that ensure the confidentiality, integrity, and availability of ePHI; protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI and unauthorized uses or disclosures of such ePHI; ensure compliance with the Security Rule by the workforce members of regulated entities, while also taking into account the technical capabilities of record systems used to maintain ePHI; the costs of such measures; the need for training users who have access to ePHI; the value of audit trails in computerized record systems; and the needs and capabilities of small and rural health care providers.

The Department has consulted with and relied on the recommendations of NCVHS in the formulation of this proposed rule[86] and intends to continue to engage in these consultations before finalizing the rule.[87] We also expect to consult with the National Uniform Billing Committee, the National Uniform Claim Committee, the Workgroup for Electronic Data Interchange, and the American Dental Association before finalizing this rule, as required by section 1172(c)(3)(A)(ii) of HIPAA.[88]

---

[86] *See* Letter from NCVHS Chair Jacki Monson (2022), *supra* note 123; Letter from NCVHS Chair Jacki Monson (2023), *supra* note 123.
[87] 42 U.S.C. 1320d–1(f).
[88] 42 U.S.C. 1320d–1(c)(3)(A)(ii).

IV. Section-by-Section Description of the Proposed Amendments to the Security Rule

This section contains a description of the proposed amendments to the Security Rule and the Department's rationale for its proposals. As part of this rationale, we often include a discussion of best practices contained in previously published guidance documents issued by the Department, NIST, and other Federal agencies. We request comment on previously published guidance documents that are not discussed herein that were issued by the Department or other Federal agencies and contain best practices but may be relevant or applicable to regulated entities, including the names of and citations for such guidance documents. We do not propose to adopt referenced best practices as the standard or implementation specifications unless otherwise specified in the proposed regulatory text. Rather, we include such discussion to provide regulated entities with context for the aforementioned proposals. We recognize that regulated entities are of varying types and sizes and may be concerned that requiring the adoption of such best practices might not be appropriate for all. However, we request comment on whether we should require implementation of certain aspects of a particular guidance document. If so, please explain which aspect(s) we should require, the rationale, and information about the burden of implementing such aspect(s).