Sweeping Changes Proposed to the HIPAA Security Rule

January 22, 2025

INSIGHTS

- For the first time in more than a decade, the government has proposed sweeping changes to the HIPAA Security Rule.
- The changes are proposed in response to concerns "regarding the state of cybersecurity in the health care industry" and "regarding the sufficiency of the security measures implemented by regulated entities."
- If finalized, the proposed changes will require both covered entities and business associates to closely review their existing systems and evaluate what additional measures might be necessary to ensure compliance.
- The proposed changes could also increase regulated entities' liability under the False Claims Act.

On January 6, 2025, the Department of Health and Human Services' (Department) Office for Civil Rights (OCR) published a Proposed Rule that, if finalized, would substantially revise the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule for the first time in more than a decade. See 90 Fed. Reg. 898 (Jan. 6, 2025).

The Proposed Rule, which spans 125 pages, seeks to address the significant changes to the environment in which "health care is provided and in which regulated entities operate … including transformative changes in how regulated entities [which include both covered entities and their business associates], create, receive, maintain, and transmit [electronic protected health information (ePHI)]." These changes would make the Security Rule significantly more prescriptive and require more proactive measures from covered entities—health care providers, health plans, and health care clearinghouses—and their business associates.

The Department will receive comments through March 7, 2025. Both the full text of the Proposed Rule and a digital form for submitting public comments online are available here.

Below, we provide a summary of some of the Proposed Rule's key changes.

Removing Distinction Between "Required" and "Addressable" Implementation Specifications to Make All Implementation Specifications Required

Since it was first issued in 2003, the Security Rule has distinguished between "addressable" and "required" implementation specifications. "Addressable" implementation specifications include, for example, procedures for protecting against malicious software, password management, log-in monitoring, automatic logoff, backup of ePHI before moving equipment, and encryption of ePHI. "While none of the implementation specifications were optional," preamble commentary to the Proposed Rule notes that "designating some of the implementation specifications as addressable provided each covered entity with the ability to determine whether certain implementation specifications were reasonable and appropriate safeguards for that entity." The Proposed Rule would do away with that distinction and make all implementation specifications "required."

Technology Asset Inventory and Network Map

The Proposed Rule would also require regulated entities to conduct and maintain an accurate and thorough written technology asset inventory, as well as a network map of its electronic information systems and all technology assets that may affect the confidentiality, integrity, or availability of ePHI. This would require regulated entities to identify their information systems that create, receive, maintain, or transmit ePHI and all technology assets, including hardware, software, electronic media, information, and data, that may affect ePHI. Moreover, the Proposed Rule would require that regulated entities determine the movement of ePHI through, into, and out its information systems and describe such movement in a network map.

If finalized, regulated entities would be required to review and update the written inventory of technology assets and network map at least annually *and* when there is a change in the regulated entity's environment or operations that may affect ePHI.

Risk Analysis

While covered entities and business associates are required to, among other things, conduct an accurate and thorough assessment of potential risks and vulnerabilities, the current regulations do not provide any specificity as to what would constitute such an accurate and thorough assessment. The Proposed Rule, in addition to "elevating" this existing requirement from an implementation specification to a standard, would require regulated entities to "conduct an accurate and comprehensive written assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI created, received, maintained, or transmitted by the regulated entity."

More particularly, the Department proposes "eight implementation specifications" for regulated entities to perform and document as part of this risk analysis:

- Review the technology asset inventory and the network map to identify where ePHI may be created, received, maintained, or transmitted within its information systems.
- Identify all reasonably anticipated threats to the confidentiality, integrity, and availability of ePHI that it creates, receives, maintains, or transmits.
- Identify potential vulnerabilities and predisposing conditions to the regulated entity's relevant electronic information systems, including electronic information systems that create, receive, maintain, or transmit ePHI or that otherwise affect the confidentiality, integrity, or availability of ePHI.
- Create an assessment and documentation of the security measures it uses to ensure that the measures protect the confidentiality, integrity, and availability of the ePHI created, received, maintained, or transmitted by the regulated entity.

- Make a reasonable determination of the likelihood that each identified threat would exploit the identified vulnerabilities.

- Make a reasonable determination of the potential impact of each identified threat should it successfully exploit the identified vulnerabilities.

- Create an assessment of risk level for each identified threat and vulnerability.

- Create an assessment of risks to ePHI posed by entering into or continuing a business associate agreement or other written arrangement with any prospective or current business associate, respectively, based on the written verification obtained from the prospective or current business associate.

Regulated entities would also be required to review, verify, and update the written assessment annually.

Patch Management

In recognition of hackers ongoing attempts "to target the health care industry in search of ways to access valuable ePHI," the Proposed Rule would create a three-tiered hierarchy of patches based on the level of risk, with accelerated deadlines for installing higher risk patches:

- 15 calendar days for a "critical risk" patch, update, or upgrade, either from the date the need for it is identified if it is already available or otherwise within 15 calendar days of it becoming available;

- 30 days from the same dates for "high risk" patches, updates, or upgrades; and

- Within a "reasonable and appropriate period of time" for all other patches, updates, or upgrades, which "would be determined by the regulated entity's written policies and procedures for identifying, prioritizing, acquiring, installing, evaluating, and verifying the timely installation of patches, updates, and upgrades."

Complying with these proposed timelines will require regulated entities to consult and engage with their IT departments on an ongoing basis.

Requiring Certain Verifications from Business Associates on an Annual Basis

The Proposed Rule would also require covered entities to obtain annually from their business associates written verification that the business associate has deployed technical safeguards required under the Security Rule. Notably, because business associates' subcontractors are themselves business associates, the Proposed Rule would require the same annual written verification from subcontractors. Additionally, the Proposed Rule would require this written verification to be accompanied by a written analysis of the business associate's relevant electronic information systems, which "would be required to be performed by a person with appropriate knowledge of and experience with generally accepted cybersecurity principles and methods for ensuring the confidentiality, integrity, and availability of ePHI." Currently, the Proposed Rule does not require that the written analysis be performed by an independent expert; in other words, if finalized as proposed, the written analysis could be performed by a member of a regulated entity's IT department possessing sufficient expertise.

Additional Security Measures

In addition to the changes summarized above, the Proposed Rule would require regulated entities to:

- Encrypt all ePHI at rest and in transit, with limited exceptions;

- Deploy anti-malware protection to prevent, detect, and contain cyberattacks;

- Deploy multi-factor authentication to verify the identity of persons seeking access to relevant electronic information systems;

- Implement a vulnerability management program that includes using a vulnerability scanner to detect vulnerabilities such as obsolete software and missing patches every six months;

- Require regulated entities with multiple, distinct electronic information systems to separate these systems using reasonable and appropriate technical controls (network segmentation);

- Require regulated entities to deploy technical controls to create and maintain exact retrievable copies of ePHI as a means of strengthening data backup and recovery.

Potential False Claims Act Risk

Since HIPAA's inception more than 2 decades ago, the Department has maintained that the Security Rule provides regulated entities with the "flexibility to choose appropriate security measures considering their size, capabilities, the costs of the specific security measures, and the operational impact, enabling them to reasonably implement the standards of the Security Rule." However, the significant changes and enhanced specificity proposed by the Department in the Proposed Rule could, in addition to increasing the risk of direct liability under HIPAA, increase regulated entities' liability under other statutes such as the federal False Claims Act.

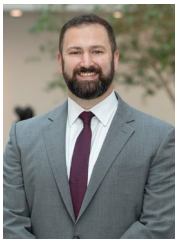
In October 2021, Deputy Attorney General Lisa O. Monaco of the United States Department of Justice (DOJ) announced the Civil Cyber-Fraud Initiative (the "Initiative") to "utilize the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients." To date, most of the cases made public under the Initiative have been premised on an entity's failure to implement a specific set of contractual cybersecurity requirements to which the entity agreed to adhere, as opposed to a theory that a regulated entity failed to comply with HIPAA and submitted false claims to a government health care program.

This could be due in large part to the existing Security Rule's flexibility. Indeed, it can be difficult to show that a regulated entity violated the Security Rule, let alone that such a violation, if known to the government, would have been material to its decision to pay a claim, thereby implicating the False Claims Act. The Proposed Rule's additional requirements and specificity, if finalized, could serve to create additional avenues through which the government or relators could bring lawsuits against regulated entities under the False Claims Act.

Please note that the information provided in this release is general in nature and not intended as legal advice. Specific circumstances may vary, and we encourage clients to contact us directly for personalized assistance and further information.

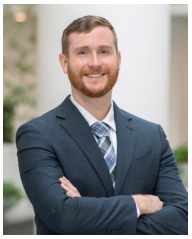
AUTHORS

Jennifer M. Vaughan
Partner
jvaughan@phrd.com
404 420 5531



David A. O'Neal
Partner
doneal@phrd.com
404 880 4755

Kristen Bond Dobson
Associate
kdobson@phrd.com
850 391 5197



Travis C. Williams
Associate
twilliams@phrd.com
404 880 4751