1/2/25 Alert 2025-01

Employee Benefits Compliance

HHS Proposes Updates to HIPAA Security Rule to Strengthen Cybersecurity for Electronic Protected Health Information ("ePHI")

Introduction

On December 27th, 2024, the Office for Civil Rights ("OCR") at the Department of Health and Human Services ("HHS" or "Department") issued a Notice of Proposed Rulemaking ("NPRM" or "Proposed Rule") designed to strengthen cybersecurity standards under the HIPAA Security Rule. Specifically, the Proposed Rule would revise existing standards with the intent to better protect the confidentiality, integrity, and availability of electronic protected health information (ePHI). The proposals would revise the Security Rule to address: (1) changes in the environment in which health care is provided; (2) significant increases in breaches and cyberattacks; (3) common deficiencies the Office for Civil Rights has observed in investigations into Security Rule compliance by covered entities and their business associates (collectively, "Regulated Entities"); (4) other cybersecurity guidelines, best practices, methodologies, procedures, and processes; and, (5) court decisions that affect enforcement of the Security Rule. The NPRM is scheduled to be published on January 6, 2025, and once published, the public will have 60 days to provide comment. Whether the rule will ultimately be finalized given the change in Administration is uncertain, but HIPAA security rules have generally not been the subject of significant debate or controversy so it is possible these rules will ultimately be finalized. Regardless, plan sponsors should be aware of these potential new requirements and consider what changes may be necessary given that certain updates may take time to implement.

Background

HIPAA's Privacy and Security Rules are made up of three interrelated but separate rules: (1) the Privacy Rule; (2) the Security Rule; and (3) the Breach Notification Rules. The Privacy Rule applies to any and all types of protected health information ("PHI") and imposes rules related to its use and disclosure. The Breach Notification Rules requires HIPAA Covered Entities and their Business Associates to provide certain notifications to impacted entities and individuals in the event of a breach of PHI. The Security Rule, on the other hand, applies *only* to electronic PHI ("ePHI"), which is individually identifiable health information ("IIHI") that is transmitted by or maintained in electronic media. Specifically, the Security Rule requires Regulated Entities to:

- protect the confidentiality, availability, and integrity of ePHI;
- protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI and unauthorized uses or disclosures of ePHI; and,
- ensure compliance with the Administrative Simplification provisions by officers and workforce members of Regulated Entities.

In order to enforce these goals, the Security Rule requires Regulated Entities to implement certain administrative, physical, and technical safeguards along with certain organizational and documentation requirements. Under the current Security Rule, each safeguard can be satisfied by implementing a series of "required" and "addressable" implementation specifications. "Required" specifications being, of course, required in order to satisfy a particular safeguard and "addressable" specifications allowing flexibility for Regulated Entities to determine whether it is reasonable and appropriate for that Regulated Entity. Where it is reasonable and appropriate, the Regulated Entity must adopt the addressable implementation specification. Where an addressable implementation specification it is not reasonable and appropriate, the Security Rule allows the Regulated Entity to adopt an alternative measure that achieves the purpose of the standard, if the alternative measure is reasonable and appropriate. In such cases, the Regulated Entity must also document why it is not reasonable and appropriate to implement the addressable implementation specification.

The Security Rule was initially published in 2003 and most recently updated in 2013. Since that time, there have been significant technological advancements that have impacted the way health care is provided and the way information is shared amongst industry stakeholders. There have also been significantly more breaches and cyberattacks in recent years. Given the evolving data security landscape, including court decisions and industry/state/local cybersecurity requirements, HHS seeks to update the existing Security Rule requirements to better reflect the current environment.

A Note on Applicability: *Note that HIPAA's Privacy and Security rules generally apply to health plans, health care clearinghouses, and health care providers ("Covered Entities") who conduct certain electronic transactions involving protected health information ("PHI") and to those entities with which they share PHI to assist with plan functions ("Business Associates"). For employer plan sponsors who only offer fully insured lines of medical coverage, the insurance carriers are generally responsible for compliance with HIPAA's Privacy and Security Rules. Where a group health plan has at least one self-funded line of medical coverage, the plan is generally responsible for compliance with the HIPAA Privacy and Security rules and this obligation generally falls to the employer/plan sponsor. While employers sponsoring fully-*

insured plans rarely have access to PHI, if they do so on a regular basis (a "hands-on" plan), which can be the case in certain states that allow plan sponsor access to fully insured medical plan data, they would likely be required to fully comply with HIPAA's Privacy and Security Rule requirements as well. For more information on the application of the HIPAA Privacy and Security Rule, see our Alliant Insight: 101 A HIPAA Foundation for Employer-Plan Sponsors.

New Security Rule Proposals

The NPRM includes a host of proposals designed to improve the confidentiality, availability, and protection of ePHI. While many of these are viewed by the Department simply as clarifications of steps Regulated Entities should already be taking to comply with the Security Rule, some are entirely new and will require modification to existing policies, procedures, training, and documentation, and may require updates in information technology (IT) security infrastructure.

Note that these proposals are highly technical and will require the involvement of an organization's IT team to fully understand and appreciate their scope, and also to implement any required changes. We provide here a simple, non-exhaustive summary of the most impactful proposals in the NPRM:

- Remove the distinction between "required" and "addressable" implementation specifications and make all implementation specifications required with specific, limited exceptions.
    - For example, encryption of ePHI has historically been categorized as an addressable implementation specification, meaning that organizations can currently perform an analysis to determine whether it is reasonable and appropriate for them to implement. If they determine it is not, then they could implement a different safeguard that they do find to be reasonable and appropriate to protect ePHI. Under the proposed rules, encryption, along with all other implementation specifications will be generally be required and Regulated Entities will no longer be able to perform this type of an analysis.
- Require written documentation of all Security Rule policies, procedures, plans, and analyses.
- Add specific compliance time periods for many existing requirements.
- Require a technology asset inventory and a network map that illustrates the movement of ePHI throughout the Regulated Entity's electronic information system(s) on an ongoing basis,

but at least once every 12 months and in response to a change in the Regulated Entity's environment or operations that may affect ePHI.

- Require greater specificity for conducting a risk analysis, including a written assessment that contains, among other things:
  - A review of the technology asset inventory and network map.
  - Identification of all reasonably anticipated threats to the confidentiality, integrity, and availability of ePHI.
  - Identification of potential vulnerabilities and predisposing conditions to the Regulated Entity's relevant electronic information systems
  - An assessment of the risk level for each identified threat and vulnerability, based on the likelihood that each identified threat will exploit the identified vulnerabilities.
- Strengthen requirements for planning for contingencies and responding to security incidents. Specifically, Regulated Entities would be required to:
  - Establish written procedures to restore the loss of certain relevant electronic information systems and data within 72 hours.
  - Perform an analysis of the relative criticality of their relevant electronic information systems and technology assets to determine the priority for restoration.
  - Establish written security incident response plans and procedures documenting how workforce members are to report suspected or known security incidents and how the Regulated Entity will respond to suspected or known security incidents.
  - Implement written procedures for testing and revising written security incident response plans.
- Require Regulated Entities to conduct a compliance audit at least once every 12 months to ensure their compliance with the Security Rule requirements.
- Require that Business Associates verify at least once every 12 months for Covered Entities (and that Business Associate contractors verify at least once every 12 months for Business Associates) that they have deployed technical safeguards required by the Security Rule to

protect ePHI through a written analysis of the Business Associate's relevant electronic information systems by a subject matter expert and a written certification that the analysis has been performed and is accurate.

- Require encryption of ePHI at rest and in transit, with limited exceptions.
- Require Regulated Entities to establish and deploy technical controls for configuring relevant electronic information systems, including workstations, in a consistent manner. New express requirements would include:
  - Deploying anti-malware protection.
  - Removing extraneous software from relevant electronic information systems.
  - Disabling network ports in accordance with the Regulated Entity's risk analysis.
- Require the use of multi-factor authentication, with limited exceptions.
- Require vulnerability scanning at least every six months and penetration testing at least once every 12 months.
- Require Regulated Entities to review and test the effectiveness of certain security measures at least once every 12 months, in place of the current general requirement to maintain security measures.
- Require Business Associates to notify covered entities (and subcontractors to notify business associates) upon activation of their contingency plans without unreasonable delay, but no later than 24 hours after activation. Business Associate Agreements should be updated to reflect this new requirement.
- Require group health plans to include certain language in their plan documents requiring plan sponsors to comply with the administrative, physical, and technical safeguards of the Security Rule and ensure that any contractor that handles plan ePHI agrees to implement the same administrative, physical, and technical safeguards, among other requirements.

Employer Impact and Next Steps

If finalized, these proposed changes will require significant updates and modifications to HIPAA security policies and procedures, as well as updates to documentation and training for workforce members responsible for handling ePHI. The NPRM proposals may also require updates to an organization's IT security infrastructure. Whether updates will be required likely depends on the sophistication of an organization's existing IT infrastructure. Most of the proposed requirements can be met by an IT security infrastructure that implements current best practices and complies with various state data privacy and security laws. Employer plan sponsors with less developed or sophisticated IT security infrastructures should review these proposed rules and (1) consider what changes might be required, and (2) develop internal resources to address the issues or seek third party support IT security support. While employers sponsoring self-funded medical plans will be most impacted by the new rule, employers sponsoring fully insured plan should also be aware of these proposals.

As noted, whether this NRPM will be finalized after the new Administration takes office is uncertain, and the Alliant compliance team will monitor the NPRM and provide an update if the proposed rules become final.