CLIENT ALERTS & INSIGHTS

OCR Proposes Modification to HIPAA Security Rule

FEBRUARY 27, 2025

Authors: Daniel S. Marks, Lauri A. Cooper, Rachit Parikh

In late December 2024, the Office of Civil Rights at the U.S. Department of Health and Human Services ("OCR") issued a notice of proposed rulemaking to modify the Security Standards to the Protection of Electronic Protected Health Information ("Security Rule") issued under the Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"). The proposed modifications are aimed at strengthening cybersecurity protections for electronic protected health information ("ePHI"). The modifications were proposed to support the nation's commitment to improving cybersecurity and infrastructure, as the number of breaches affecting 500 or more individuals reported to the OCR have grown at an alarming rate.

Justification for Proposed Rulemaking

The proposed rule includes several express justifications underlying the modifications. First, OCR determined that strong security standards are essential for protecting ePHI and ensuring quality and efficiency of the nation's healthcare system. A recent survey found that 92% of healthcare organizations surveyed had experienced a cyberattack, and three-quarters of the respondents who experienced a cyberattack reported that there were negative effects on patient care. For example, a recent ransomware attack caused a level 1 trauma center to go without access to its electronic health records system ("EHRs") for 25 days and ultimately resulted in a significant loss of ePHI. According to OCR, the frequency and severity of cyberattacks demonstrate that planning and preparing for data breaches and potential cyberattacks is extremely important.

In addition, OCR determined that the healthcare environment has continued to change since the Security Rule was last revised in 2013. Specifically, the healthcare environment has shifted to rely more on interconnected information systems to maintain and exchange patient health information. For example, hospitals more frequently use (i) EHRs[1] and other electronic record and billing systems that maintain ePHI, (ii) software for telemedicine delivery with patients, and (iii) medical devices and equipment connecting patients and providers to networks, all of which are susceptible to cyberattacks. Further, the emergence of artificial intelligence in the healthcare field increases the risks and vulnerabilities to ePHI within information systems.

OCR has also found that compliance with the requirements of the current Security Rule is inconsistent and that most healthcare- covered entities fail to implement Security Rule requirements that include conducting risk analysis consisting of a thorough analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI which are fundamental to protecting ePHI. Further, covered entities also fail to create and implement compliance response plans for security incidents. By issuing this proposed rule, OCR intends to clarify steps that covered entities and their business associates must take to adequately protect ePHI.

Summary of Key Proposed Modifications

The proposed rule codifies actions that health plans, healthcare clearinghouses, and most healthcare providers and their business associates (collectively "Regulated Entities") need to take to adequately protect PHI and ePHI. The proposed rule further: (a) clarifies that the Security Rule applies to all ePHI; (b) amends "addressable" obligations to "required" obligations, with the result that all elements of the Security Rule are "required" unless a specifically identified exception applies; (c) revises certain definitions and adds new definitions to reflect current technology used by Regulated Entities; (d) clarifies certain existing requirements; and (e) adds entirely new requirements to reflect technological advancements and evolutions to best practices since the last updates to the Security Rule. The proposed rule focuses on key changes for 1) Administrative Safeguards, 2) Physical Safeguards, and 3) Technical Safeguards required under the Security Rule.

1. Administrative Safeguards. OCR proposed changes to Administrative Safeguards in the Security Rule, requiring Regulated Entities to:
   - Prepare a thorough written technology asset inventory and network map of its electronic information systems and all technology assets that may affect the confidentiality, integrity, or availability of ePHI to better identify systems that create, receive, maintain, or transmit ePHI.
   - Produce both written technical and nontechnical evaluations, including evaluating whether changes in the Regulated Entity's environment affect the confidentiality, integrity, or availability of ePHI and to perform such evaluations in a reasonable time period before making a change to its environment (e.g., adopting new technology assets, upgrading, updating, or patching technology assets, recognizing new threats, etc.).
   - Timely apply patches and update configurations to software and firmware for all devices used by Regulated Entities and develop patch management written policies and procedures and review such written policies and procedures once every twelve months.
   - Implement security awareness and training standards on protection of ePHI at least once every twelve months.
   - Perform audits of compliance with each standard and implementation specification of the Security Rule at least once every twelve months.

2. Physical Safeguards. OCR proposed changes to Physical Safeguards in the Security Rule, including requiring Regulated Entities to:
   - Implement written policies and procedures related to facility access control, including describing physical access to the Regulated Entity's electronic information systems.
   - Implement written policies and procedures for the use of workstations, including any workstation that accesses ePHI (e.g., mobile devices).
   - Implement written policies and procedures for the removal of technology assets.

3. Technical Safeguards. OCR proposed changes to Technical Safeguards in the Security Rule, including requiring Regulated Entities to:
    - Restrict access to electronic information systems only to those users and technology assets that have been expressly granted access and assign a unique identifier to track every technology asset.
    - (i) Implement technical controls to encrypt and decrypt all ePHI in accordance with widely accepted standards, (ii) encrypt ePHI in transit and at rest, and (iii) review and test the effectiveness of the encryption-related technical controls at least once every twelve months or in response to environmental or operational changes.
    - Implement technical controls for configuring electronic information systems (e.g., workstations, software used), which are reviewed at least once every twelve months, including deploying anti-malware protection, removing extraneous software, and disable unsecured network ports.
    - Implement multi-factor authentication for all technology assets in its relevant electronic information systems.
    - (i) Perform vulnerability scans at least once every six months, (ii) perform penetration testing at least once every twelve months, and (iii) review and test the effectiveness of the technology asset that performs the automated vulnerability scan every twelve months.
    - (i) Create copies of ePHI so that copies are no more than 48 hours older than the ePHI maintains in the electronic information systems, (ii) deploy technical controls to create and maintain backups, and (iii) test the technical controls at least once every six months.

Next Steps

The proposed rule is receiving comments until March 7, 2025, which may be submitted by the general public here. Once the final rule is issued, it will be effective 60 days from publication in the federal register. Regulated Entities must be compliant within the compliance date (proposed as 180 days from the effective date). However, the proposed rule includes an additional transition period[2] to allow Regulated Entities time to update their business associate agreements to include the new provision that requires a business associate to report to its covered entity the activation of a contingency plan within 24 hours.

Overall, the goal of the proposed changes is to require Regulated Entities to implement stronger security controls and procedures to better protect ePHI from data breaches. Based on the number of discreet changes that are contained in the proposed rule, Regulated Entities may be required to make significant modifications to their existing security practices when the new rule goes into effect.

Benesch HIPAA and privacy attorneys will continue to review the proposed rule and its impact on Regulated Entities and assist clients in maintaining compliance with the rule as it is finalized and implemented.

[1] While use of EHRs by health care providers is not strictly required, the HITECH Act and the 21st

Century Cures Act created financial incentives and penalties for provider adoption and meaningful use of EHR.

[2] Specifically, OCR is proposing a transition period of (1) the date such contract is renewed on or after the compliance date of the final rule or (2) a year after the effective date of the final rule, whichever is earlier.

Daniel Marks is a Partner in the firm's Intellectual Property Practice Group. He may be reached at 216.363.6101 or dmarks@beneschlaw.com.

Lauri Cooper is Of Counsel in the firm's Healthcare+ Practice Group. She can be reached at 216.363.4678 or lcooper@beneschlaw.com.

Rachit Parikh is a Managing Associate in the firm's Intellectual Property Practice Group. He can be reached at 312.212.4966 or rparikh@beneschlaw.com.