BOCHNER PLLC
1040 Avenue of the Americas, 15TH Floor, New York, NY 10018
o 646.971.0685 e law@bochner.law w bochner.law

Health and Human Services Proposes Stronger HIPAA Cybersecurity Rules

Quick Tips and Need to Know

- HHS has proposed changes to the HIPAA Security Rule to strengthen cybersecurity protections for electronic health information ("ePHI") by altering the existing Security Rule's requirements for (1) documentation and policy, (2) technical and physical safeguards, and (3) compliance and auditing.
- The current rule will remain in effect while HHS undertakes rulemaking.
- Public comments on the proposed rule are due on March 7, 2025

HHS Releases Notice of Proposed Rulemaking to address Cybersecurity of ePHI

On December 27, 2024, the Office for Civil Rights (OCR) of the Department of Health and Human Services (HHS) issued a notice of proposed rulemaking to enhance cybersecurity protections for electronic protected health information. The proposed rule is part of the Department's larger effort to address cybersecurity risks in the healthcare sector by enhancing cybersecurity of patient data. *See* Healthcare Sector Cybersecurity: Introduction to the Strategy of the U.S. Department of Health and Human Services.

Concerns about cybersecurity risks in the healthcare industry are not unfounded –in 2024, major health systems such as Kaiser Permanente, Change Healthcare, and Ascension, were targets of cyberattacks on patient healthcare data. In response to growing cybersecurity risks, HHS proposes to amend existing protections under HIPAA and the HITECH Act to create national standards for cybersecurity protections of electronic protected health information (ePHI). The proposed rule would alter existing requirements under the HIPAA Security Rule for a regulated entity's (1) documentation and policy protocols, (2) technical and physical safeguards, and (3) compliance and auditing procedures.

Industry Impact

The proposed rule has not been adopted and entities who are subject to HIPAA and the HITECH Act should continue adhering to the existing HIPAA security rule. Importantly, the public will have until March 7, 2025, to submit comments on the proposed rule. Once comments have been received, HHS will work to further amend the rule to address public concerns flagged during the comment period. At this time, we encourage healthcare entities to remain attentive to the proposed rule's comment period and monitor the HHS website for continued guidance on standards for addressing cybersecurity risks. For more information on the HIPAA security rule or the proposed changes, please contact Matthew Shatzkes, matthew@bochner.law, Jonathan Rogoff, jonathan@bochner.law, or Bessie Frías, bfrias@bochner.law.

Proposed Changes:

I. Documentation and Policy Requirements

HHS would require Regulated Entities to:

- Maintain written documentation of all Security Rule policies, procedures, plans, and analyses.

- Establish written procedures to restore the loss of certain relevant electronic information systems and data within 72 hours.

- 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.

- Require business associates to 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 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.

- Require group health plans to include in their plan documents requirements for their group health plan sponsors to:
    - Comply with the administrative, physical, and technical safeguards of the Security Rule.
    - Ensure that any agent to whom they provide ePHI agrees to implement the administrative, physical, and technical safeguards of the Security Rule.
    - Notify their group health plans upon activation of their contingency plans without unreasonable delay, but no later than 24 hours after activation.

II. Technology and Security Safeguard Requirements

HHS would require Regulated entities to:

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

- 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.

- Use multi-factor authentication, with limited exceptions.
- Conduct vulnerability scanning at least every six months and penetration testing at least once every 12 months.
- Segment networks
- Maintain separate technical controls for backup and recovery of ePHI and relevant electronic information systems.

III. Compliance and Auditing Requirements

HHS would require Regulated Entities to:

- Conduct a compliance audit at least once every 12 months to ensure their compliance with the Security Rule requirements.
- 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.
- Notify HHS within 24 hours when a workforce member's access to ePHI or certain electronic information systems is changed or terminated.
- Develop and revise technology asset inventory and a network map that illustrates the movement of ePHI throughout the regulated entity's electronic information system(s), at least once every 12 months and in response to a change in the regulated entity's environment or operations that may affect ePHI.