Proposed Amendments to HIPAA Security Rule: What's Ahead

4/22/2025

Proposed Amendments to HIPAA Security Rule

The U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) published in the January 6, 2025 Federal Register a Notice of Proposed Rulemaking titled "HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information" (NPRM), which was initially released in December 2024. We previously wrote about the NPRM in our January 27, 2025 Healthcare Law Alert. The NPRM proposes to substantially amend the HIPAA Security Rule due to, in relevant part, significant increases in breaches and cybersecurity attacks and common deficiencies found by the OCR during its investigations into compliance by covered entities and their business associates. The proposed amendments, if finalized as written, would place substantial enhanced security requirements and, resultingly, significant human resources and financial burdens on covered entities and business associates. The public comment period for the NPRM closed on March 7, 2025. HHS is now in the process of categorizing and reviewing the comments received and, typically, next steps would be to publish a final rule that may contain amendments from the original NPRM after taking into consideration the public comments.

Industry Group Resistance to and Criticism of Proposal as Written

On February 17, 2025, a number of industry groups sent a letter to President Trump and the Secretary of HHS "to express our unified opposition to the proposed HIPAA Security Rule." The industry groups cited several reasons for their position, including that the "combination of the depth and breadth of the proposed requirements on an unreasonable timeframe presents significant challenges... and would place an undue financial strain on hospitals and healthcare systems" and that the rule would stifle healthcare innovation. Last month, the Health Sector Coordinating Council, Cybersecurity Working Group (HSCC CWG)

published a Statement on Healthcare Cybersecurity Policy (Statement). The HSCC CWG is a government-recognized critical infrastructure industry council of more than 470 healthcare providers; lab, blood, pharmaceutical and medical technology companies; payers; health IT entities; public health and government agencies partnering to identify and mitigate cyber threats to patient care, health data and research, systems, and manufacturing.

In the Statement, the HSCC CWG outlined the almost 30 leading practices and guidance documents produced by the working group, including a comprehensive set of cybersecurity controls published in 2019 and updated in 2023, and "initiatives and recommendations that measurably improve our cyber defenses and resiliency to protect patient safety." With respect to the NPRM, the HSCC CWG stated that the proposed rule "either dismisses these important developments or mischaracterizes their potential for measurable improvement. A considerable number of the 52 CWG member industry associations that submitted comments representing their constituent members have made their concerns clear in their submissions to HHS about the cost and complexity of implementing the rule and the dubious effectiveness that compliance could achieve at improving security." Ultimately, the HSCC CWG "advises that the Administration suspend any further consideration of the NPRM as written and initiate a structured series of consultations and workshops with the HSCC CWG and other owners and operators of our national critical healthcare infrastructure to forge consensus on a modernized policy for healthcare cybersecurity resiliency, responsibility and accountability."

Path Forward

Resultingly, it is unclear whether HHS will follow the typical route of considering the comments to the NPRM and publishing a final rule in due course, or if it will engage in the consultative process recommended by the HSCC CWG prior to publishing the final rule. What is clear, though, is that the OCR continues to take seriously its Security Rule Risk Analysis Initiative and continues to investigate and take action against covered entities and business associates who have experienced cyberattacks, including ransomware attacks, resulting from insufficient security controls and monitoring. The OCR recently announced the settlement of its 7th enforcement action in its Risk Analysis Initiative and of its 11th ransomware enforcement action. What is also clear is that cyberattacks, including ransomware attacks, continue to vex the healthcare industry and the business associates servicing the industry. Covered entities and business associates should take advantage of the substantial available security guidance and take measures to enhance compliance with the Security Rule and improve overall security programs.

How We Can Help

If you have questions or would like assistance with your data privacy and security program, contact:

Lani M. Dornfeld, Esq., CHPC, *Member,* Healthcare Law at 973.403.3136 or ldornfeld@bracheichler.com

Authors

The following attorneys contributed to this insight.

Lani M. Dornfeld

CHPC, Member
Healthcare Law

973.403.3136 · 973.618.5536 Fax

ldornfeld@bracheichler.com