

Publications

Proposed Update to the HIPAA Security Rule

Related Attorneys

Jolie N. Havens
J. Liam Gruzs
Christopher L. Ingram
Sydney N. Pahren
Nikkia Knudsen
Jennifer Bibart Dunsizer
Margaret "Peggy" M. Baron
Jacquelyn Meng Abbott
Elizabeth Howard
Rylee R. Snively

Related Services

Data Strategy, Privacy and Security

Related Industries

Health Care

CLIENT ALERT | 1.24.2025

In early January, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) published a Notice of Proposed Rulemaking. The Proposed Rule would modify the Security Standards for the Protection of Electronic Protected Health Information (Security Rule) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). This proposal aims to strengthen cybersecurity requirements for electronic protected health information (ePHI) in response to increasing cybersecurity threats to the health care sector. This is the first significant update to the Security Rule in more than ten years. Below is an overview of important proposed changes and clarifications.

Implementation Requirements and Compliance Timelines

HHS has identified various gaps in the current cybersecurity framework and proposed revisions to definitions to better reflect current technology and terminology. Implementation specifications will now be required, with limited exceptions.

Administrative and Technical Safeguards

The proposed rule also outlines administrative requirements for conducting a risk assessment, including an inventory of technology assets and the development of a network map. Technical safeguard requirements include vulnerability scanning, threat assessment, network segmentation, anti-malware deployment, disabling network ports, encrypting ePHI at rest and in transit, and requiring multi-factor authentication.

Incident Response and Vulnerability Organization

Regulated entities must enhance their security incident procedures and response plans. For instance, the rule establishes contingency plan requirements, including a 72-hour system restoration time. Annual contingency planning effectiveness tests will also be required along

with enhanced data backup protocols and recovery practices.

Business Associate and Group Health Plan Considerations

While the proposal impacts all regulated entities, some of the rules are specific to Business Associates and Group Health Plans. Business Associates must provide written verification to Covered Entities that technical safeguards have been deployed. They must also notify Covered Entities within 24 hours of activating any contingency plans. Group Health Plans must ensure agents receiving ePHI implement administrative, physical, and technical safeguards and, like Business Associates, notify their group health plans within 24 hours of activating contingency plans.

The Proposed Rule, which can be found [here](#), outlines a variety of additional changes, aligning HIPAA with current trends and industry standards. Comments to the proposed rule are due on March 7, 2025. Once the Proposed Rule is finalized, it will take effect 60 days after publication and regulated entities must comply no later than 180 days after the final rule effective date. It is unclear what impact, if any, the [January 20, 2025, Executive Order](#) implementing a regulatory freeze pending review will have on this rule.

For further information about the Proposed Rule, its implications, or assistance with submission of comments, please reach out to your Vorys attorney.