National Rural Health Association

HIPAA Security Rule – Proposed Rule to Strengthen Cybersecurity for ePHI

The Department of Health and Human Services (HHS), through its Office for Civil Rights (OCR), has issued a proposed rule to modify the HIPAA Security Rule. An HHS press release can be found here.

Comments on the proposed rule are due within 60 days of its publication in the Federal Register and may be submitted via regulations.gov. Please see below for the main provisions:

Background: The HIPAA Security Rule establishes national standards to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI). **Health plans, health care clearinghouses, and any health care providers that transmit information electronically ("regulated entities") are subject to the Security Rule and any proposed updates.**

Since the last update to the Security Rule in 2013, the healthcare sector has seen exponential growth in cyberattacks, with over 167 million individuals affected by breaches in 2023 alone, a 102% increase since 2018. This proposed rule seeks to address modern cybersecurity threats, aligning with the Biden-Harris Administration's National Cybersecurity Strategy and HHS's Healthcare Sector Cybersecurity initiatives.

Proposed changes: The proposed updates to the HIPAA Security Rule aim to strengthen cybersecurity protections and clarify compliance requirements for covered entities, including health care providers. These include:

- **Making all implementation specifications mandatory**, with limited exceptions. Implementation specifications are the standards required by the Security Rule.
    - Currently, implementation specifications are either required or addressable. Required implementation specifications are mandatory while addressable specifications give flexibility to providers to decide whether it is reasonable and appropriate for them to implement.
- **Requiring regulated entities to maintain written documentation for all policies**, procedures, risk analyses, and plans.
- Requiring the development and revision of a technology asset inventory and a network map that illustrates the movement of ePHI throughout the regulated entity's electronic information systems on an ongoing basis, but at least once every 12 months.
- Adding, modifying, and clarifying definitions used in regulations to better reflect the current health care environment.
- Adding new, more specific requirements for risk analyses conducted by regulated entities.
- **Requiring penetration tests at least every 12 months and vulnerability scanning at least every 6 months.**
- **Mandatory encryption of ePHI with limited exceptions** and use of multi-factor authentication (MFA) to access ePHI systems. New technical measures will also be mandated, including use of anti-malware protection, disabling unused network ports, and removing unnecessary software from systems to reduce vulnerabilities.
- Bolstering incident response and contingency planning requirements. **Regulated entities must establish written security incident response plans**, outlining processes for reporting and handling

incidents. Additionally, regulated entities must have a written plan to restore electronic information systems and data within 72 hours of a breach.

- **Introducing mandatory audits and testing.** Regulated entities will be required to conduct annual compliance audits and test the effectiveness of their security measures. Vulnerability scanning must occur every six months, with penetration testing conducted at least annually.

These proposed changes collectively reflect an effort to modernize the Security Rule, address emerging cybersecurity challenges, and enhance the resilience of the healthcare sector. **Rural health care providers are not exempt from the provisions in the proposed rule.** HHS notes that it is critical for small, rural providers to comply as they are especially high-risk targets for a security breach**. However, HHS also clarifies that rural providers can determine the security measures that are most reasonable and appropriate to use in order to comply with standards and implementation specifications. The proposed rule specifically asks for comments regarding whether the proposed rule sufficiently accounts for the needs and capabilities of rural providers.**

If you have any questions on the proposed rule, please contact Alexa McKinley Abel (amckinley@ruralhealth.us).