Proposed HIPAA Security Rule Updates

BDO

STRENGTHENING CYBERSECURITY PROTECTIONS FOR EPHI: A NEW ERA FOR THE HIPAA SECURITY RULE

On December 27, 2024, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) issued a Notice of Proposed Rulemaking (NPRM) to amend the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule.
This proposed rule aims to bolster cybersecurity protections for Electronic Protected Health Information (ePHI) amidst escalating cyber threats targeting the healthcare sector. This initiative is part of a broader commitment to enhance the cybersecurity of critical infrastructure, as outlined in the National Cybersecurity Strategy.

THE IMPERATIVE FOR CHANGE

The healthcare sector is increasingly vulnerable to cyberattacks, which can compromise sensitive patient data and disrupt critical services. A recent survey found that 92 percent of surveyed health care organizations had experienced a cyberattack in the past year[1], and almost 75% of these respondents noted negative effects on patient care[2]. Healthcare organizations continue to be the targets of cybercriminals given their successful attack rate and overall financial gain. Breach costs in the healthcare industry continue to be the highest, with an average cost of $10.1M[3]. At an individual level, those affected by a medical record breach and who had their identity compromised, incurred an average cost of $13,500 to deal with the breach[4].

HHS has specifically called out their concerns related to the number of breaches/cybersecurity incidents, the upward trend of affected individuals, and the potential harm this will cause to those affected individuals[5]. The proposed modifications to the HIPAA Security Rule reflect a proactive approach to these threats, so that covered entities and business associates—comprising health plans, healthcare clearinghouses, healthcare providers, and their service providers—are better equipped to safeguard ePHI.

Key provisions of the proposed rule can be categorized into five categories:

Information security program | **Risk management and compliances** | **Data inventorying/mapping** | **Incident response and contingency planning** | **Third-party risk management**

Not all of the potential requirements within the categories are equal in terms of complexity and level of implementation effort, and we have highlighted our perspective on the impactful items within each category.

Full proposed rule: https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-ruleto-strengthen-the-cybersecurity-of-electronic-protectedhealth-information

Notice Fact Sheet: https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html

1: "The 2024 Study on Cyber Insecurity In Healthcare: The Cost and Impact on Patient Safety and Care," Ponemon Institute, p. 3 (2024) (The report, sponsored by Proofpoint, Inc., included survey responses from 648 IT and IT security practitioners at U.S.-based health care organizations.).
2: Letter from NCVHS Chair Jacki Monson (2023), supra note 123, p. 5
3: "Cost of a Data Breach Report 2023," IBM, p. 13 (2023), https://www.ibm.com/reports/data-breach.
4: "An Insight into the Current Security Posture of Healthcare IT: A National Security Concern," supra note 130, p. 3.
5: See "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information," Office for Civil Rights, U.S. Department of Health and Human Services, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

INFORMATION SECURITY PROGRAM

The proposed rule requires the implementation of an information security program including several key technical controls such as:

1. **Network Segmentation and Technical Controls:** The proposed rule requires network segmentation and the deployment of consistent technical controls across electronic information systems, enhancing security architecture and reducing the potential blast radius of cybersecurity breaches. Network segmentation can be incredibly challenging given the complex interconnectivity of an organization's technology ecosystem, especially if systems were not implemented with this requirement in mind during their onset. Understanding these connectivity dependencies and engineering retrofitted segmentation can require a level of effort that includes technology, processes, policies, and personnel.
2. **Encryption and Multi-Factor Authentication:** Encryption of ePHI at rest and in transit becomes mandatory, alongside the implementation of multi-factor authentication, with specific exceptions related to legacy tech that does not support MFA and/or emergency situations. These measures are critical in preventing unauthorized access to sensitive data.
3. **Regular Vulnerability Assessments:** Entities must conduct vulnerability scanning every six months and penetration testing annually, for continuous monitoring and mitigation of potential security threats.
4. **Timely Access Notifications:** Regulated entities must notify relevant parties within 24 hours of changes or terminations in workforce access to ePHI.

RISK MANAGEMENT AND COMPLIANCE

The proposed changes provide additional requirements for conducting an annual HIPAA security risk analysis and include the following:

1. A review of the technology asset inventory and network map.
2. Identification of all reasonably anticipated threats to the confidentiality, integrity, and availability of ePHI.
3. Identification of potential vulnerabilities and predisposing conditions to the regulated entity's relevant electronic information systems.
4. An assessment of the risk level for each identified threat and vulnerability, based on the likelihood that each identified threat will exploit the identified vulnerabilities.

The proposed rule also eliminates the distinction between "required" and "addressable" implementation specifications, mandating all specifications with limited exceptions. This change aims to create a uniform standard across the board. Additionally, organizations are required to conduct an annual compliance assessment to evaluate their compliance with the Security Rule requirements.

DATA INVENTORYING AND MAPPING

The proposed rule mandates the development and regular updating of a technology asset inventory and network map, illustrating the flow of ePHI. This requirement is intended to produce a comprehensive understanding of data storage and movement and associated risk throughout the enterprise. Inventorying data and mapping its lifecycle can be challenging given continuous changes throughout the business and technology landscape. This requires both a "top-down" and "bottom-up" data governance/discovery approach. The "top-down" approach includes interviewing business and technology stakeholders to understand their ePHI processing activities, data usage, and data lineage. The "bottom-up" approach includes implementing automated technology solutions to discover and catalogue ePHI throughout the environment that may be missing or misrepresented during the "top-down" discussions. This is especially challenging when ePHI is stored in unstructured formats.

INCIDENT RESPONSE AND CONTINGENCY PLANNING

Strengthened requirements for incident response and contingency planning include:

1. Completing restoration of critical systems and data within 72 hours of a disruption for continuity of care and service delivery. While three (3) days may seem like ample time to recover key systems, recovery during a continuity event can be a complex task with sometimes hundreds of dependencies. This proposed rule requires technical investment to host resilient systems and infrastructure and the resource attention and focus to prioritize technical backup controls and associated testing. Appropriate testing can also be a resource-intensive exercise and technically challenging given system architecture.
2. Establishing detailed incident response plans and procedures for a swift and coordinated response during a potential cybersecurity incident.
3. Implementing testing and revision protocols for these plans so they are complete and accurate. And to exercise the recovery muscle to increase effectiveness and efficiency during an actual recovery event.
4. Conducting criticality analyses to prioritize system restoration so recovery efforts are focused on an appropriate direction.
5. Establishing technical controls for backup and recovery to enhance data integrity and availability.

THIRD-PARTY RISK MANAGEMENT

The rule introduces stringent requirements for business associates, including:

1. Annual verification of technical safeguards by subject matter experts to determine business associates maintain the appropriate controls to protect the confidentiality, integrity, and availability of ePHI. While many organizations will have vendor risk assessment processes in place, this proposed requirement will place a greater focus on a business associate's expertise, capabilities, credentials, and the discrete requirement of subject matter expertise signoff. This will likely require changes to vendor risk assessment processes, contractual clauses, and broader business associate cybersecurity practices.
2. Prompt notification to covered entities upon activation of contingency plans to enable covered entities to take immediate action to mitigate potential business disruptions/respond to cybersecurity incidents. This would include incorporation of applicable Incident Response and Contingency Planning based on the impact of the third-party to the organizations business.
3. Inclusion of Security Rule compliance requirements in group health plan documents to foster a culture of compliance and accountability.

OVERALL IMPLICATIONS FOR THE HEALTHCARE SECTOR

The proposed changes to the HIPAA Security Rule represent a significant shift towards more robust cybersecurity practices. By mandating comprehensive security measures and fostering accountability among regulated entities and their business associates, the rule aims to mitigate the risks posed by cyber threats.

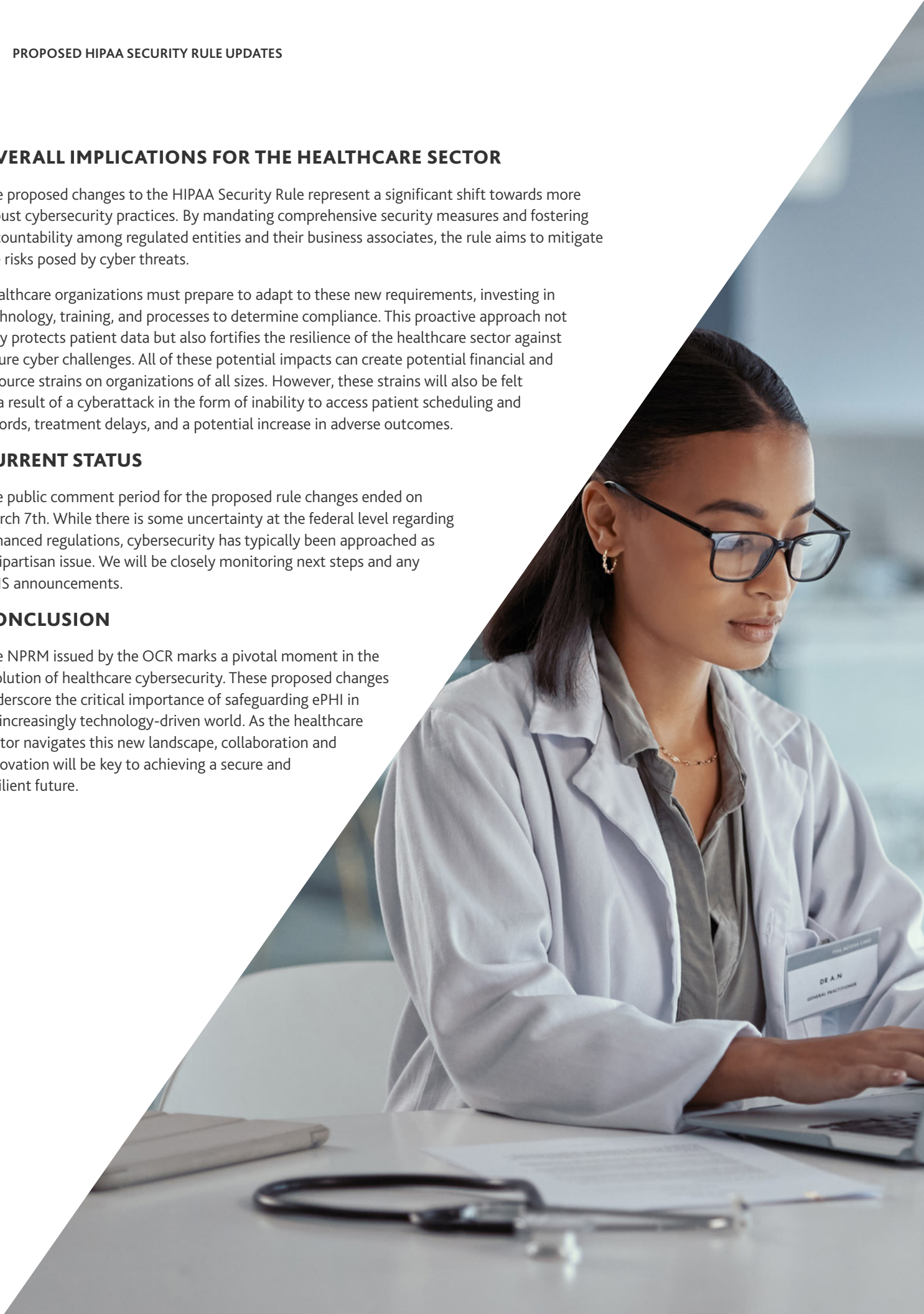
Healthcare organizations must prepare to adapt to these new requirements, investing in technology, training, and processes to determine compliance. This proactive approach not only protects patient data but also fortifies the resilience of the healthcare sector against future cyber challenges. All of these potential impacts can create potential financial and resource strains on organizations of all sizes. However, these strains will also be felt as a result of a cyberattack in the form of inability to access patient scheduling and records, treatment delays, and a potential increase in adverse outcomes.

CURRENT STATUS

The public comment period for the proposed rule changes ended on March 7th. While there is some uncertainty at the federal level regarding enhanced regulations, cybersecurity has typically been approached as a bipartisan issue. We will be closely monitoring next steps and any HHS announcements.

CONCLUSION

The NPRM issued by the OCR marks a pivotal moment in the evolution of healthcare cybersecurity. These proposed changes underscore the critical importance of safeguarding ePHI in an increasingly technology-driven world. As the healthcare sector navigates this new landscape, collaboration and innovation will be key to achieving a secure and resilient future.



HAVE QUESTIONS OR WANT TO LEARN MORE? **CONTACT US!**

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.