Published on *The National Law Review* https://natlawreview.com

AI Meets HIPAA Security: Understanding HHS's Risk Strategies and Proposed Changes

Article By:

Amy S. Leopard

Adriante Carter

In this final blog post in the Bradley series on the HIPAA Security Rule notice of proposed rulemaking (NPRM), we examine how the U.S. Department of Health and Human Services (HHS) Office for Civil Rights interprets the application of the HIPAA Security Rule to artificial intelligence (AI) and other emerging technologies. While the HIPAA Security Rule has traditionally been technology agnostic, HHS explicitly addresses security measures for these evolving technology advances. The NPRM provides guidance to incorporate AI considerations into compliance strategies and risk assessments.

AI Risk Assessments

In the NPRM, HHS would require a comprehensive, up-to-date inventory of all technology assets that identifies AI technologies interacting with ePHI. HHS clarifies that the Security Rule governs ePHI used in both AI training data and the algorithms developed or used by regulated entities. As such, HHS emphasizes that regulated entities must incorporate AI into their risk analysis and management processes and regularly update their analysis to address changes in technology or operations. Entities must assess how the AI system interacts with ePHI considering the type and the amount of data accessed, how the AI uses or discloses ePHI, and who the recipients are of AI-generated outputs.

HHS expects entities to identify, track, and assess reasonably anticipated risks associated with AI models, including risks related to data access, processing, and output. Flowing from the proposed data mapping safeguards discussed in previous blog posts, regulated entities would document where and how the AI software interacts with or processes ePHI to support risk assessments. HHS would also require regulated entities to monitor authoritative sources for known vulnerabilities to the AI system and promptly remediate them according to their patch management program. This lifecycle approach to risk analysis aims to ensure the confidentiality, integrity, and availability of ePHI as technology evolves.

Integration of AI developers into the Security Risk Analysis

More mature entities typically have built out third-party vendor risk management diligence. If finalized, the NPRM would require all regulated entities contracting with AI developers to formally incorporate Business Associate Agreement (BAA) risk assessments into their security risk analysis. Entities also would need to evaluate BAs based on written security verifications that the AI vendor has documented security controls. Regulated entities should collaborate with their AI vendors to review technology assets, including AI software that interacts with ePHI. This partnership will allow entities to identify and track reasonably anticipated threats and vulnerabilities, evaluate their likelihood and potential impact, and document security measures and risk management.

Getting Started with Current Requirements

Clinicians are increasingly integrating AI into clinical workflows to analyze health records, identify risk factors, assist in disease detection, and draft real-time patient summaries for review as the “human in the loop.” According to the most recent HIMSS cybersecurity survey, most health care organizations permit the use of generative AI with varied approaches to AI governance and risk management. Nearly half the organizations surveyed did not have an approval process for AI, and only 31% report that they are actively monitoring AI systems. As a result, the majority of respondents are concerned about data breaches and bias in AI systems.

The NPRM enhances specificity in the risk analysis process by incorporating informal HHS guidance, security assessment tools, and frameworks for more detailed specifications. Entities need to update their procurement process to confirm that their AI vendors align with the Security Rule and industry best practices, such as the NIST *AI Risk Management Framework*, for managing AI-related risks, including privacy, security, unfair bias, and ethical use of ePHI.

The proposed HHS requirements are not the only concerns clinicians must consider when evaluating AI vendors. HHS also has finalized a rule under Section 1557 of the Affordable Care Act requiring covered healthcare providers to identify and mitigate discrimination risks from patient care decision support tools. Regulated entities must mitigate AI-related security risks and strengthen vendor oversight in contracts involving AI software that processes ePHI to meet these new demands.

Thank you for tuning into this series of analyzing the Security Rule updates. Please contact us if there are any questions or we can assist with any steps moving forward.

Please visit the HIPAA Security Rule NPRM and the HHS Fact Sheet for additional resources.

National Law Review, Volume XV, Number 65