Mar 12, 2025

Categories:

Publications

Authors:

Barbara Bennett

Brooke Bishop

Proposed HIPAA Security Rule Requires AI Governance

In terms of healthcare data breaches, 2024 was the worst year ever, with the records of at least 53% of the U.S. population involved and two of the biggest healthcare data breaches of 2024 ranking in the top 10 of all time. In 2024 alone, there were 13 data breaches involving more than 1 million healthcare records—including the largest-ever healthcare data breach that affected an estimated 100 million individuals.

To combat this increase in cyberattacks and threats, in late 2024, the Department of Health and Human Services (HHS) issued a Notice of Proposed Rulemaking (NPRM) to modify the Security Rule under the Health Insurance Portability and Accountability Act of 1996 as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (collectively, HIPAA). The proposed modifications would revise existing standards to better protect the confidentiality, integrity, and availability of electronic protected health information (ePHI) and also for the first time address artificial intelligence (AI) systems.

This article describes briefly how healthcare covered entities and business associates can integrate the NPRM requirements into an overall AI governance program.

Why This Security Rule Update Is Important for AI

As the use of AI is becoming more common in healthcare—from being used in diagnostics and treatment to transcribing encounters with patients in real time—it is crucial for regulated entities to consider how AI will use and maintain ePHI to ensure it is being properly secured.

Although AI can be extremely beneficial, its growth has led to the concern of mass-scale cyberattacks. One example of these attacks is called "offensive AI," which is an attack code able to mutate as it learns about its environment. These mutations make the codes less likely to be detected and harder to stop. After assessing current and potential threats associated with AI, HHS directed several updates in the NPRM toward the HIPAA Security Rule's application to AI, including ePHI in AI training data, prediction models, and algorithm data that is maintained by a regulated entity.

Proposed Changes Impacting AI

As a part of the NPRM, relative to AI, HHS proposes to require that regulated entities:

- Develop a written inventory of technology assets. Specifically, HHS would expect that AI software used to create, receive, maintain, or transmit ePHI or that interacts with ePHI, including where ePHI is used to train the AI software, would be listed as part of its technology asset inventory, which feeds into the regulated entity's risk analysis.
- Consider the type and amount of ePHI accessed by any AI tool, to whom the data is disclosed, and to whom the output is provided when conducting risk analysis and management activities. (The HIPAA Security Rule suggests referencing the National Institute of Standards and Technology's (NIST) AI Risk Management Framework as a helpful resource for regulated entities to better understand and measure the risks associated with AI.)
- Conduct repeated risk analyses that consider the effects of changes on the confidentiality, integrity, and availability of ePHI.
- Monitor authoritative sources for known vulnerabilities, remediate those vulnerabilities in accordance with their patch management program and apply patches, updates, and upgrades that address critical and high risks promptly.

Steps Regulated Entities Can Take Now to Prepare

These AI-related NPRM requirements emphasize the need for a robust AI governance program to manage AI risks. Regulated entities can begin to prepare for compliance with these proposed updates by taking the following steps:

- Ensure your business adopts an enterprise-wide AI governance program.
- Review any current AI governance program, including risk analysis and management procedures, to compare the processes you currently have in place with the requirements under the NPRM.
- Compile a list of all the current AI tools that your entity uses, what the tools are used for, how they access data (including ePHI), what that data is used for, and how the data is stored. Once this list has been created, ensure that all AI tools and use cases are addressed by your current AI governance program. If you notice any gaps, immediately develop a plan to address them.

For guidance on the development of a scalable AI governance program, see ***Three Steps to AI Success for CEOs*** and ***New Expectations for AI: Governance is Key for AI Success in Health Care***. For considerations around the use of ePHI to train or prompt an AI model, see ***Beware Privacy Risks In Training AI Models With Health Data*****.**

FBT has a sophisticated and experienced healthcare AI team to provide guidance and assist in complying with the NPRM and the development of AI guardrails, including a enterprise-wide AI governance program. Please reach out to the authors of this article or your contacts on Frost Brown Todd's Health Care Innovation team.

AI Legally Speaking

Explore the collection of articles below for more AI-related coverage and legal analysis.

- ***Managing Data Security and Privacy Risks in Enterprise AI***
- ***New Expectations for AI: Governance is Key for AI Success in Health Care***
- ***USPTO Guidance Suggests Two Strategies for AI Inventions***
- ***FTC's New Rule on Consumer Reviews: Ensuring Compliance with Human- and AI-Generated Content***
- ***Decoding Colorado's Artificial Intelligence Act***
- ***Investment Management + AI = New Opportunities, Unique Risks***
- ***AI and Energy: Network Innovation and Growth***
- ***AI and Health Care Providers: Managing the Risks with Data***
- ***Using Generative AI in Manufacturing: Three Key Considerations***
- ***Will AI Destroy the DMCA Copyright Compromise?***
- ***Three Steps to AI Success for CEOs***

Learn More