AI in Health Care: What Privacy Officers Need to Know to Remain HIPAA Compliant

Article
Amundsen Davis Health Care Alert
December 2, 2025

Artificial intelligence (AI) is everywhere you look now, boasting an ability to streamline workflow and boost efficiency—and the health care industry is no exception. Whether used for billing, patient care, or diagnostic purposes, AI tools are being regularly utilized by health care professionals and hospitals. As covered entities under HIPAA, providers must ensure their adoption of these tools remains compliant with their privacy, security, and regulatory obligations.

Evolving Regulations

In January 2025, the Department of Health and Human Services (HHS) published a proposed rule to revise HIPAA's Security Rule requirements to protect against breaches and cyberattacks.

The rule would establish that electronic protected health information (ePHI) used in AI training data, prediction models, and algorithm data that is maintained by a regulated entity for covered functions is protected by HIPAA. It will require heightened risk analysis and risk management activities, including a written inventory of a covered entity's technology assets that includes AI software that creates, receives, maintains, transmits, or interacts with ePHI, and regular monitoring of authoritative sources for known vulnerabilities and prompt remediation in accordance with patch management programs.

The rule will also apply to AI use by business associates. This is in addition to the final rule HHS published earlier this year for business associates setting requirements aimed at improving transparency about design development, training, evaluation, and use of predictive decision support interventions (DSIs), which are a subset of AI that relies on machine learning and other models to support clinical decision making.

The notice of proposed rulemaking also included a request for information regarding new and emerging technologies, including AI, indicating potential for more proposed rule changes in the near future. Although some thought the proposed rule may not become final, it is on HHS's official regulatory agenda for

PROFESSIONALS

Bailee Brown
Associate

RELATED SERVICES

Health Care

AMUNDSEN DAVIS

May 2026.

In addition to these federal changes, every state has introduced legislation related to AI. Twelve states have enacted legislation related to its use in health care.

Risks of Noncompliance

While HIPAA has no private right of action, covered entities can be held liable for noncompliance by HHS's Office for Civil Rights and state attorneys general. Civil penalties include fines up to $50,000 per violation, including for unknown violations. Criminal penalties for knowing violations range from imprisonment for one to 10 years and fines from $50,000–$250,000.

Covered entities also risk reputational harm. A recent whistleblower lawsuit against Verily, a subsidiary of Alphabet, alleged the company failed to report more than 25,000 known HIPAA violations. This comes at the same time Verily has restructured to focus on data and AI, resulting in an 80 percent drop in its valuation.

Takeaways to Stay Compliant

Privacy officers should consider reevaluating current processes to determine whether:

1. **Risk management protocols are sufficient.** Conduct regular risk management audits to ensure data integrity and adjust security measures as needed.
2. **Contracts need modifications.** Review existing business associate agreements for any potential changes needed due to incorporating AI into your practitioners' or facilities' practices.
3. **AI servers are private.** Ensure data input into machine learning programs is properly limited in scope and only utilized with AI tools that use encrypted, internal servers. Public server AI tools (such as ChatGPT) do not comply with HIPAA's Privacy and Security Rules.

Subscribe to Amundsen Davis's Health Care Updates: