Briefings on HIPAA

HIPAA Q&A: AI, telehealth, and new HIPAA rules that matter now

by Rebecca Herold, CDPSE, FIP, CISSP, CIPM, CIPP/US, CIPT, CISM, CISA, FLMI

Q: How are recent advancements in artificial intelligence (AI) and machine learning (ML) impacting the management of patient data privacy, and what best practices should HIPAA compliance officers implement to address these challenges?

A: AI and ML show great promise for bringing benefits to the provision of healthcare. However, before using AI/ML tools, every healthcare provider needs to first ensure that the tools have security and privacy capabilities built within them, and that they have been comprehensively tested for things such as mitigating unauthorized PHI data use and sharing, identifying bias in results, identifying algorithmic inaccuracies, etc.

A key privacy problem is using real patient data to train AI. Typically, when a healthcare provider uses an AI tool to support patient care, that data is also being used at the same time to train the AI tool—a tool that may be utilized in many other healthcare organizations. Lack of security and privacy controls could then lead to other covered entities (CE) gaining unauthorized access to the PHI used to train the tools. This is a common problem with using AI-supported chatbots to answer patient questions via apps, websites, and other types of interactive tools.

Additionally, most organizations using such tools do not realize that the AI tool provider is a business associate (BA) due to access to PHI. Providers, and other types of CEs, are obligated to ensure all their BAs are complying with HIPAA requirements; this is for all of the Security Rule, Breach Notification Rule, and Privacy Rule requirements that apply to the associated BA based upon their services/products.

Before using AI/ML tools, all CEs need to check to ensure the following:

- Verify that the CE's data will not be used by the vendor/BA to train the AI/ML tools for use in other organizations, and that the data will not be shared with any other organization.
- Use synthetic data (whenever possible), which is generated data that mimics the characteristics of real patient data without being tied to actual patients.
- Ensure that any data—approved by the appropriate, authorized role—to use outside of the organization has been fully de-identified using one of the two methods HIPAA specifically indicates are acceptable:
  - Expert determination (generally, certification of de-identification by an outside expert).
  - HIPAA de-identification safe harbor method (removal of all 18 PHI identifiers, which include information also often found publicly online, including name, dates, city, state, ZIP code, and age).
- Verify the AI/ML tools have been rigorously tested with the broadest of possible inputs, and have been determined to be accurate and not result in unacceptably biased results.
- Establish and consistently follow procedures to obtain fully transparent, clear, and explicit consent from patients to use their data for AI/ML processing. The consent forms should include explanations describing how the patient data will be used for AI research. Keep all signed consents in a central, secured, access-controlled location and retain them for at least six years, in accordance with HIPAA requirements.
- Strongly encrypt all PHI used for AI/ML purposes and implement effective access controls to protect data from unauthorized access, which would be a violation of HIPAA and would trigger the activation of breach response plans, including notifying patients whose PHI was involved.
- Regularly audit and perform risk assessments for the AI/ML systems and procedures to identify any vulnerabilities and HIPAA compliance infractions.
- Monitor the AI/ML systems, to identify unauthorized access attempts for access, change management activities, authorized access to PHI used within AI/ML tools to support maintaining an accounting of disclosures as well as provide access logs that may be needed for incident response and breach investigations, and other activities supporting HIPAA requirements.
- Provide regular training on security and privacy policies and procedures, and ongoing reminders and communications, to all personnel using AI/ML tools and their associated PHI.

Q: With the rise of telehealth services post-pandemic, what measures should healthcare organizations take to ensure HIPAA compliance and protect patient information in virtual environments?

A: Telehealth is going to continue expanding in use given the increasing healthcare deserts being created throughout many regions of the U.S. as healthcare providers leave areas, especially rural areas, where funding is being cut for hospitals and clinics.

Another factor widening these healthcare deserts is states enacting laws limiting healthcare services and putting

healthcare providers in legal jeopardy when treating patients. Healthcare workers are simply choosing not to work in those states.

This makes establishing specific security and privacy protections in telehealth ecosystems critically important, not only for HIPAA compliance, but also to help provide care and protect the associated patients.

Generally, telehealth platforms and associated vendors are BAs of the healthcare providers, who are CEs, using the platforms. As such, BAs are required to comply with all the HIPAA Security Rule and Breach Notification Rule requirements. Telehealth providers also have the applicable Privacy Rule requirements they must comply with, or at least support the compliance efforts of their CE clients.

Here is a high-level checklist for healthcare providers to help ensure they are implementing necessary measures to stay compliant with HIPAA security and privacy requirements:

- Assign a role (individual, team, or department) responsible for managing, monitoring, and maintaining HIPAA compliance within the organization's telehealth ecosystem.
- Ensure the telehealth BA agreements (BAA) detail the required data security protocols and ensure the software meets HIPAA's technical, physical, and administrative safeguards. Also, ensure BAAs include the specific activities from the Privacy Rule that the BA must support, such as providing a quick and uncomplicated method for access to patient PHI in support of the HIPAA Privacy Rule Right of Access requirements.
- Do not allow BAs to use telehealth data to train any AI/ML tool they use, unless the assigned CE role has authorized such use and contractually established the circumstances within which such data is authorized for use, with the implementation of security and privacy requirements for how the data is to be used, shared, retained, destroyed, etc.
- Ensure the CE's business ecosystem has security and privacy controls built within the full breadth of the telehealth ecosystem that support compliance with HIPAA security, privacy, and breach response requirements.
- Update policies, procedures, forms, and processes involving telehealth activities to include security and privacy actions specific to telehealth.
- Provide regular training for telehealth security and privacy policies and procedures, along with ongoing awareness reminders.
- Perform regular risk assessments for the telehealth ecosystem: at least once a year (often as part of the overall risk assessment for the organization), when major changes involving telehealth occur, and following breach mitigation activities.

Providers should also educate their patients on securing their PHI wherever it is located (the environment within their vicinity where telehealth activities occur, the security of their personal computing devices, etc.) through to the CE's telehealth ecosystem components (the patient's authentication credentials, etc.).

HHS provides a good resource for telehealth security and privacy for patients. They also provide some useful advice for CEs.

Q: How should compliance leaders navigate the complexities of data sharing and interoperability initiatives while maintaining strict adherence to HIPAA regulations?

A: Create and maintain a PHI directory that documents all the sources of PHI within the CE, and the recipients of PHI leaving the CE. It should include associated details such as how the PHI is protected throughout different point-to-point transmission paths (e.g., type of encryption), the purposes for the data sharing, the locations and types of repositories for PHI storage, and the applications used with the PHI.

By documenting and keeping current these basic yet critical information items, compliance leaders will be able to more efficiently, effectively, and expeditiously support legitimate and authorized data sharing while staying in compliance with HIPAA.

CEs may also benefit by working with an information sharing and analysis organization to stay up to date with current and emerging threats to their PHI.

A few common threat sources include:

- Natural threats: Tornadoes, derechos, floods, earthquakes, hurricanes, tropical storms, electrical storms, landslides, avalanches, forest fires, etc.
- Human threats: Events enabled by or caused by human beings, whether unintentional (mistakes, inadvertent data entry, lack of awareness due to lack of training, etc.) or deliberate (network-based attacks, malicious software infections, unauthorized access to confidential information, etc.).
- Environmental threats: Long-term power failures, building safety compromise, pollution, chemicals, liquid leaks, electrical fires, etc.
- Digital threats: Denial of service attacks, ransomware, viruses, unauthorized activity monitoring, etc.

Q: What are the most significant changes in the 2024 updates to HIPAA regulations, and how should compliance officers prioritize their efforts to align with these new requirements?

A: The first major change occurred on April 22, when the HIPAA Privacy Rule to Support Reproductive Health Privacy was announced. This final rule strengthens the HIPAA Privacy Rule by prohibiting the disclosure of PHI related to reproductive healthcare in certain circumstances.

It prohibits the use or disclosure of PHI: 1) to investigate or impose liability on individuals, healthcare providers, or others who seek, obtain, provide, or facilitate reproductive healthcare that is lawful under the circumstances in which such healthcare is provided; or 2) to identify persons for such activities.

It also requires a regulated healthcare provider, health plan, or clearinghouse (or their BAs) to obtain a signed attestation that certain requests for PHI potentially related to reproductive healthcare are not for these prohibited purposes. It additionally requires regulated healthcare providers, health plans, and clearinghouses to modify their Notice of Privacy Practices to support reproductive healthcare privacy.

This second big change from 2024 was the April implementation of the Confidentiality of Substance Use Disorder (SUD) Patient Records final rule. This new rule increases coordination among providers treating patients for SUDs, strengthens confidentiality protections through civil enforcement, and enhances integration of behavioral health information with other medical records to improve patient health outcomes.

The rule also:

- Permits use and disclosure of 42 *CFR* Part 2 records based on a single patient consent given once for all future uses and disclosures for treatment, payment, and healthcare operations
- Permits redisclosure of Part 2 records by HIPAA CEs and BAs in accordance with the HIPAA Privacy Rule, with certain exceptions
- Provides new rights for patients under Part 2 to obtain an accounting of disclosures and to request restrictions on certain disclosures, as also granted by the HIPAA Privacy Rule
- Expands prohibitions on the use and disclosure of Part 2 records in civil, criminal, administrative, and legislative proceedings
- Provides HHS enforcement authority, including the potential imposition of civil money penalties for violations of Part 2
- Outlines new breach notification requirements applying to Part 2 records

CEs and BAs should determine which of these new rules have the most impact upon their organizations, and then prioritize implementing the new requirements. For each of the new rules, CEs and applicable BAs will need to do the following:

- Update their security and privacy policies and procedures to incorporate the new reproductive health and SUD data requirements and procedures
- Provide training to all personnel with responsibilities involving SUD data, covering the new requirements and following up with ongoing awareness communications
- Perform audits and risk assessments to ensure the associated controls are in place and working as intended

Editor's note: Herold is CEO of Privacy & Security Brainiacs, a provider of cybersecurity and risk management training, assessment, and SaaS solutions.