Briefings on HIPAA

HIPAA compliance tips and news roundup

by Dom Nicastro

It's been a busy year for HIPAA. Here's the latest roundup of compliance tips and news to digest as we head toward the final third of the year.

Comprehensive risk assessment for ePHI

Anurag Lal, CEO of NetSfere and former director of the U.S. National Broadband Task Force (part of the Federal Communications Commission), caught up with **BOH** for a security discussion. We asked him to give a comprehensive approach to conducting a risk assessment for ePHI that aligns with the NIST SP 800-66r2 guidelines.

Risk assessments, Lal says, should be implemented for the healthcare enterprise. To be productive endeavors, they should include all of the following steps:

- Ask where ePHI is created, received, maintained, processed, and transmitted. Identify where ePHI is generated within the organization, where and how it enters the organization, where it moves and flows within the organization (e.g., specific information systems), where it is stored, and where it leaves.
- Identify the threats, potential vulnerabilities, and predisposing conditions.
- Determine the likelihood that a threat will exploit a vulnerability and the impact of such an event.
- Determine the level of risk.
- Document the risk assessment results.

Risk assessments will hopefully lower the need for risk management.

"By implementing safe and secure technology platforms, healthcare entities can avoid [extra] risk management, especially when it comes to protecting ePHI," Lal says. "The healthcare systems must train employees as well. Employee training and education is a critical part of any enterprise rollout of technology and ePHI. Ongoing training and education should help employees understand both the benefits and the risks associated with the handling of ePHI."

For effective workforce security, Lal says enterprises must ensure all employees understand the organization's cybersecurity risks and are educated on how to communicate or transport ePHI properly.

"The enterprise must identify where the ePHI is generated, where it ends, where it moves, where it is stored, and where it leaves the organization," Lal adds. "This includes all systems: mobile devices, medical equipment, and IoT devices."

Employees should periodically take inventory and check for updates on hardware and software, understand the configuration of the organizational systems, and perform a business impact analysis. Creating and implementing a risk management program is best practice for upholding technical safeguards.

Organizations must also look at their policies, procedures, and risk management activities to ensure compliance with the HIPAA Security Rule and NIST guidance. This begins with assigning clear job roles and descriptions and ensuring they are communicated throughout the organization, according to Lal.

"Healthcare entities need to make certain that workforce members are equipped with the necessary knowledge, skills, and abilities to fulfill particular roles and that these requirements are included as part of the personnel hiring process," Lal says. "However, training should be an ongoing, evolving process in response to environmental and operational changes. While roles and responsibilities are assigned, there should be checks and balances to ensure all requirements are met and there are no risks of ePHI."

NIST SP 800-66r2 was just published in February, but organizations in 2024 continue to face basic challenges with the HIPAA Security Rule. Many healthcare entities are unaware of the technologies or platforms they're using, resulting in Security Rule noncompliance as well as fines, Lal says.

"The healthcare industry should be implementing technologies with true end-to-end encryption that are HIPAA compliant," he adds.

To ensure effective workforce security, technologies need to be fully encrypted, protecting sensitive data at rest and in transit, according to Lal. "Using true encryption," he adds, "enterprises can protect sensitive business information from unauthorized access or theft, and this is one of the best ways to prevent data breaches."

Another best practice is working to avoid human error. Regular cybersecurity training is a must for employees who are increasingly targeted by cybercriminals, according to Lal.

“With regular training, employees can become a powerful defense against cyberthreats,” Lal says. “Cybersecurity training will educate employees on the importance of security and staying in compliance with HIPAA. And making this a regular occurrence will keep employees updated on evolving security best practices and threats.”

Given the rapid evolution of threats to ePHI security, organizations must ensure their security measures are up to date.

OCR imposes civil monetary penalty of $115,200

On August 1, 2024, OCR announced a civil monetary penalty of $115,200 against American Medical Response (AMR), a national provider of emergency medical services. This penalty stems from an investigation prompted by a complaint that AMR failed to provide a patient with timely access to their medical records.

Under the HIPAA Privacy Rule, individuals or their personal representatives are entitled to access their health information within 30 days, with a possible 30-day extension, for a reasonable, cost-based fee.

This action marks OCR's 49th enforcement of the HIPAA Right of Access provision.

“HIPAA gives patients a right to timely access to their medical records,” said OCR Director Melanie Fontes Rainer in the announcement. “OCR will continue to enforce this right through investigations, and when necessary, by imposing civil money penalties.”

As privacy leaders know, the HIPAA Privacy Rule establishes national standards for the protection of medical records and sets limits on the use and disclosure of PHI. It also grants individuals rights, including that of timely access to their health records.

The investigation into the complaint revealed that AMR failed to provide the patient with timely access to their medical records despite the patient trying multiple times to obtain access. In response to OCR's findings, AMR sent the patient a copy of their records and revised its internal procedures to improve the tracking and processing of access requests.

In October 2023, OCR issued a Notice of Proposed Determination to impose the penalty. AMR waived its right to a hearing and did not contest the findings, leading to the finalization of the penalty.

Update to OCR’s Change Healthcare cybersecurity incident FAQ webpage

On July 19, Change Healthcare reported a ransomware attack that resulted in a breach of PHI. The initial breach report identified approximately 500 individuals affected, which is the minimum number required for posting on the HHS Breach Portal. Change Healthcare is still assessing the total number of individuals impacted, and the HHS Breach Portal will be updated if the count changes.

The HIPAA breach report form on the HHS Breach Portal allows for amendments, enabling filers to update initial reports or add additional information.

OCR has also updated the answer to question 3 on the "Change Healthcare Cybersecurity Incident Frequently Asked Questions" webpage to address this situation and will continue to provide updates as needed.

On February 21, 2024, Change Healthcare detected ransomware in its computer system and immediately took steps to halt the attack, including disconnecting and shutting down systems to prevent further damage. The company launched an investigation and notified law enforcement, while its security team, supported by top experts, worked to address the incident and determine its scope. Change Healthcare has found no evidence that the ransomware spread beyond its own systems.

By March 7, the company confirmed that a significant amount of data had been exfiltrated from its environment between February 17 and February 20. On March 13, Change Healthcare received a data set of exfiltrated files deemed safe for investigation and began a preliminary targeted analysis. Following this analysis, on April 22, Change Healthcare publicly confirmed that the impacted data could actually affect a substantial number of people.

HIPAA security conference

OCR and the NIST Information Technology Laboratory announced the return of the Safeguarding Health Information: Building Assurance through HIPAA Security 2024 conference. After a five-year hiatus, the conference will be held October 23–24 at the HHS headquarters in Washington, D.C.

The conference will delve into the current healthcare cybersecurity landscape and the HIPAA Security Rule. It will provide practical strategies and techniques for implementing the HIPAA Security Rule, which sets federal standards to protect the confidentiality, integrity, and availability of ePHI.

Topics will include managing cybersecurity risk, practical cybersecurity solutions, current cybersecurity threats to the healthcare sector, cybersecurity considerations for IoT in healthcare, and updates from federal healthcare agencies.

Commentary on reproductive healthcare and privacy

The final rule "HIPAA Privacy Rule to Support Reproductive Health Care Privacy" aims to safeguard sensitive health information in the wake of the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*. The Court's landmark ruling has far-reaching implications for access to abortion, particularly in states with restrictive reproductive healthcare laws, prompting a critical need for enhanced privacy protections.

The final rule, which modifies the HIPAA Privacy Rule, took effect on June 25, 2024, and organizations are expected to comply with almost all of its provisions by December 22, 2024 (the exception being 45 *CFR* 164.520, which has a compliance date of February 16, 2026). It introduces new prohibitions on the use and disclosure of PHI associated with reproductive healthcare.

Martin Gasparian, owner and attorney at Maison Law, says organizations can comply with the new rule by updating their privacy policies, conducting regular compliance audits, and integrating access controls and restrictions.

Sending regular updates to staff will guide them on abiding by the new limits related to reproductive healthcare rights and privacy.

HIPAA compliance leaders can introduce new attestation protocols to manage requests. This involves setting up a centralized request unit, implementing standard operating procedures and developing new processes to ensure that requests for PHI adhere to the updated regulations. By creating standardized request forms and automated checklists, organizations can ensure that all requests for PHI are compliant and not made for prohibited purposes, according to Gasparian.

Compliance leaders should review and update the Notice of Privacy Practices (NPP) document to make proper changes, Gasparian says.

“The adjustments of the NPP [should] integrate new requirements to enhance clarity for the staff and patients,” he says. “Proactive communication with staff and patients is vital to ensure healthcare organizations comply with final rule changes to HIPAA, protecting reproductive healthcare privacy rights.”