Briefings on HIPAA

HIPAA Q&A: Reproductive healthcare, Change breach, CISO skills

by Julia Huddleston, CIPP/US, CIPM, CCSFP

Q: What are the takeaways for HIPAA compliance officers in the HIPAA Privacy Rule to Support Reproductive Health Care Privacy final rule?

A: The HIPAA Privacy Rule to Support Reproductive Health Care Privacy, which goes into effect June 25, 2024, aims to strengthen HIPAA privacy protections by "prohibiting the disclosure of protected health information (PHI) related to lawful reproductive health care in certain circumstances."

Previously, medical record privacy was at risk, particularly when patients sought legal reproductive healthcare across state lines. The new level of HIPAA privacy includes the following provisions:

- "Prohibits the use or disclosure of PHI when it is sought 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 to identify persons for such activities."
- "Requires a regulated healthcare provider, health plan, clearinghouse, or their business associates, to obtain a signed attestation that certain requests for PHI potentially related to reproductive health care are not for these prohibited purposes."
- "Requires regulated healthcare providers, health plans, and clearinghouses to modify their Notice of Privacy Practices (NPP) to support reproductive healthcare privacy."

Compliance with the final rule is required 180 days after the effective date, which means organizations must be compliant by December 23, 2024. The Office for Civil Rights (OCR) is allowing a deferred date for required NPP changes of February 16, 2026, to accommodate other recent regulatory changes that impact NPPs. OCR has also stated that it will make available a model attestation no later than December 23, 2024.

In the meantime (and remembering that December is the height of the holiday season), covered entities (CE) should:

- Review and revise current policies and procedures regarding PHI disclosures, in addition to business associate agreements, to ensure they comply with the final rule
- Begin updating employee trainings when appropriate to help employees understand the new rule and obtain necessary attestations before disclosing PHI potentially related to reproductive healthcare

Q: HHS created an FAQ about the Change Healthcare breach. What lessons can providers learn from this breach?

A: After HHS posted its FAQ, the *Wall Street Journal* reported in late April that several issues led to the incident. These included:

- Credentials were compromised for an application that allowed Change staff members to remotely access the network
- Multifactor authentication (MFA) reportedly wasn't activated on the program
- The cybercriminals moved "laterally" as they lurked in the network, suggesting they had ample time to steal from the company's massive troves of data

In other words, basic security controls such as MFA were not in place or were somehow bypassed. This is one of the endpoint protections that HHS points to as an "essential goal" of its voluntary Cybersecurity Performance Goals. Essential goals form a floor of cybersecurity protections, per HHS (e.g., audit logging, monitoring, and incident handling).

These requirements have been part of the HIPAA Security Rule since it became effective in 2005 and are basic information security hygiene. They mean (non-technically) that every transaction needs to create a log of who did what when; those logs need to be monitored, and organizations need to be able to detect and respond to security incidents as they occur (e.g., geo-blocking).

An organization of the size and scope of Change shouldn't be ignoring basic information security—and neither should your organization. Even prior to the Change incident, it was clear that OCR had decided that 2024 was the year to enforce the HIPAA Security Rule.

In early May 2024, the OCR director confirmed in an interview that during the next seven months the agency will

restart HIPAA audits, focusing on the Security Rule (particularly risk analysis and risk management), and that a Notice of Proposed Rulemaking to update the Security Rule will be released by the end of the year. It's time to make sure that your security house is in order!

Q: In April, HHS released new guidance to reiterate and clarify hospital requirements for informed consent from patients as it relates to medical professionals performing sensitive examinations, particularly on patients under anesthesia. What's important to know for providers?

A: On April 1, HHS published a memorandum to state survey agency directors and sent a letter about the memorandum to teaching hospitals and medical schools. A few days earlier, OCR posted an FAQ to clarify hospitals' informed consent and privacy obligations to patients during examinations or procedures conducted for educational and training purposes.

This flurry of guidance is in response to reports of patients under anesthesia who were improperly examined, including pelvic, breast, prostate, and rectal examinations, without proper informed consent. These examinations were conducted as part of medical students' courses of training.

In the memorandum, HHS makes clear that permission for sensitive exams is "an essential part of the informed consent process for hospitals, and necessary for compliance with the informed consent requirements in the CMS hospital [*Conditions of Participation*]."

The new FAQ explains individuals' right under the HIPAA Privacy Rule to request that covered entities (CE) restrict the use and disclosure of their PHI for treatment, payment, or healthcare operations, and the obligation of CEs to comply with restrictions to which they agree except in emergencies. By way of example, the FAQ notes that an individual concerned about medical trainees observing a pelvic exam without their consent while they are unconscious may request their healthcare provider not to disclose their PHI to medical trainees.

If the covered healthcare provider agrees to the request, the provider may not disclose the individual's PHI to medical trainees (even if they are members of the provider's workforce). This means that, in that instance, medical trainees could not be in the room with, observe, or provide care to the individual or otherwise access the individual's PHI except in an emergency. And, in the event of an emergency, the CE would be permitted to use or disclose only the portion of the restricted PHI that is needed to provide emergency treatment.

The letter to teaching hospitals and medical schools makes a point to note that OCR investigates complaints alleging that PHI was used or disclosed to medical trainees in violation of HIPAA. The letter also emphasizes that OCR will continue to ensure CEs' policies and practices related to sensitive examinations do not discriminate against patients on any basis protected by federal civil rights laws.

Q: We are hiring a chief information security officer (CISO). What are the top traits and skills they should have?

A: A good CISO almost has to work like an oracle, seeing threats and opportunities before they actually happen. That said, top traits of a good CISO include:

- **Technical background:** CISOs should understand how technology can be used to protect data, networks, and systems. They should also be familiar with current threats and vulnerabilities, as this enables them to design and implement a security infrastructure that is effective and up to date.
- **Effective communication skills:** CISOs should be good communicators and able to clearly explain security concerns to senior management and other stakeholders. They also need to be able to translate complex security concepts into language that non-technical personnel can understand.
- **Effective managerial skills:** CISOs need to be skilled at managing and motivating teams of security professionals and engaging other members of the organization. They should understand the importance of creating a positive work environment and providing adequate resources for their team.
- **Proactiveness:** A successful CISO needs to take steps to prevent cyberattacks before they happen. They must be informed about current threats and vulnerabilities and have a plan to deal with them.
- **Resourcefulness:** A good CISO understands that not all organizations have the same budget for security and is able to prioritize according to their company's needs.
- **Innovative thinking:** A good CISO is innovative and always looking for new ways to improve their organization's security posture.
- **Strategic planning:** Good CISOs think strategically about the security of their organization. Security needs and requirements have to align with the company's business goals. Security decisions must be consistent with the organization's overall operations and vision.

Editor's note: Huddleston is Apgar and Associates' principal. She holds the designations of Certified Information Privacy Manager, Certified Information Privacy Professional, and Certified (HITRUST) CSF Practitioner. She works with Apgar & Associates' clients on certification readiness, compliance assessments, security risk analysis, and policy and procedure review and implementation. She joined Apgar & Associates in September 2010 after nearly 25 years of state

government management.