Health Information Compliance Alert

HIPAA: Bypass HIPAA Blunders With These Tips

Don't move HIPAA to the back burner.

You might be wondering if the feds still take basic HIPAA privacy and security violations seriously. The answer is yes, and you should be preparing now for a post-pandemic ramp-up.

Background: Over the past year, much of the HHS Office for Civil Rights (OCR) enforcement has focused heavily on health equity, discrimination, and Right of Access violations. But that doesn't mean that the feds aren't looking at other cases. The number of violations in the queue is substantial, and it takes time for OCR to complete investigations and reach settlements.

For example, OCR settled a HIPAA security violation with Peachstate Health Management, LLC, doing business as AEON Clinical Laboratories (Peachstate) for $25,000 in April. The initial audit of Peachstate's compliance problems dated back to December 2017, but the settlement with the clinical lab didn't occur until 2021, an OCR release shows.

After years of Security Rule mismanagement and "systemic noncompliance," Peachstate agreed to pay the penalty and enter into a "robust" corrective action plan (CAP), which includes three years of OCR monitoring, the agency says.

Appreciate the Nuances of the HIPAA Rules

It's not surprising that many organizations are challenged to fully understand the HIPAA Privacy and Security Rules, says **Melissa Dill**, product management leader for the healthcare consulting practice at Crowe.

"I think there are always challenges with deeply understanding the actual HIPAA [Privacy] Rule," Dill explains. "It is very complex. It has largely remained intact from its original implementation. There were related updates made to the HITECH Act in 2009, and now there are additional changes that were proposed in December of 2020. Often, it's a lack of familiarity with the original HIPAA Rule, as well as the changes that have come since then."

Covered entities (CEs) should keep in mind that there are two familiar parts to HIPAA, Dill says. "There's the Privacy Rule, which tends to be more focused on the non-electronic and access aspects of an individual's protected health information [PHI], and then there's a Security Rule, which focuses on the electronic management of that individual's information."

Important: The HIPAA Privacy and Security Rules offer organizations guidance on how best to set up policies and implement procedures to assess risks, protect PHI/ePHI, and circumvent violations. The rules advise not only on the provisions of the federal law, but also provide practices with guidelines to assist with HIPAA compliance planning.

Another regulation of critical concern is the HIPAA Breach Notification Rule, which doesn't always get as much attention as it should and is interwoven with the Privacy and Security Rules. This third rule focuses primarily on what organizations must do after a breach happens. Even though the Breach Notification Rule stipulates specific notification requirements post-breach, practices would be wise to review the mandates in their initial HIPAA compliance planning phases.

Why? OCR continues to view CEs and their business associates (BAs) with documented HIPAA compliance plans more favorably, and that includes having a detailed incident response scheme in place.

Privacy Rule Violations Run the Gamut From Minor to Massive

When it comes to the Privacy Rule, violations vary in intensity, from minor violations to serious ones. Dill points to

common issues like "simple things such as physicians' handwritten notes being left somewhere where they can be seen by individuals who don't have a need to see those notes, things being printed out and left on a printer for others to see, or an individual calling an office and wanting information and perhaps not being the patient, but being a patient's parent, daughter, or child who does not have permission to access such records."

She cautions, "Those sorts of things that you don't necessarily think of as an issue are the easy things to have a compliance issue or a violation."

Invest in Strong HIPAA Security or Pay the Price

On the side of the Security Rule, physician practices must have the appropriate security measures in place to protect their systems, Dill advises. "Are they investing in the technology and resources to monitor compliance and protect electronic health records in their practice?" she asks.

If practices are investing in that technology and resources, they should confirm that they're investing in the right tools that will protect them from breaches, or from cybersecurity incidents, Dill reminds. "Those have to be very seriously considered. All you have to do is go online and search 'cybersecurity breaches in healthcare,' and it will bring up a laundry list."

HIPAA Penalties Remain Serious and Steep

If you thought HIPAA fines and audits are a thing of the past, think again. "They are very real," Dill charges. Last year "was a very busy year for the OCR to investigate these breaches, and there was one settlement in 2020 that was $6.85 million, which was the second-largest in history."

In 2020, OCR publicized the following HIPAA violations, Dill says:

- A data breach stemming from a provider's dispute with a business associate: $100,000 settlement
- A health system employee stole a laptop: $1 million settlement
- An insurance company had a HIPAA breach that impacted the private information of over 10 million people: $6.85 million fine
- A medical practice's electronic health record was hacked, exposing the information of over 200,000 people: $1.5 million fine
- A multispecialty clinic refused to give a patient their medical records: $15,000 fine
- A physician services provider refused to give medical records to the parents of a minor: $10,000 fine

"Many of these fines are for physician practices, and several are related to access to a person's record," Dill maintains. "And then there were times when something was lying around in the office and someone forgot there was private information included - those things are important to monitor."

Remember: If you aren't worried about a fine as low as $10,000, think about how many E/M visits it would take for you to earn that much money. For instance, you'll collect about $92 every time you report 99213 (Office or other outpatient visit for the evaluation and management of an established patient, which requires a medically appropriate history and/or examination and low level of medical decision making. When using time for code selection, 20-29 minutes of total time is spent on the date of the encounter).

Therefore, you'd have to perform 109 level-three office visits to pay that fine, which would take up about 36 hours of the physician's time.