Eli's Rehab Report

HIPAA: Take These Steps Now to Avoid Fallout From A Required Breach Report

Spot the HIPAA compliance trend and prepare.

You may not have a choice about reporting a HIPAA breach, but you do have a choice in how you present your case so that you don't attract further scrutiny.

Recent settlements with **Lahey Hospital and Medical Center and Triple-S Management Corp.** "were the outgrowth of privacy breaches that these entities had reported to OCR, which, in turn, triggered further investigations by the agency," noted partner attorney **Laurie Cohen** in a Dec. 7 blog posting for **Nixon Peabody.** "In both cases, the OCR investigations uncovered 'widespread noncompliance' with the HIPAA Rules."

Takeaway: These cases are "a reminder that when investigating a breach, OCR may look beyond the particular incident and review the covered entity's or business associate's overall compliance with HIPAA," warned attorneys **Elizabeth Hodge** and **Thomas Range** of **Akerman** in a Dec. 1 analysis. And the next round of HIPAA audits will begin in early 2016, which will only increase the scrutiny of covered entities' and business associates' compliance efforts.

Follow this advice from Hodge and Range to make sure a breach notification doesn't lead to a punishing Corrective Action Plan and exorbitant settlement:

- Review the recent HHS Office for Civil Rights settlement agreements stemming from breach reports to determine whether your policies and procedures adequately address device security in the OCR's eyes.
- Assess whether you need to update your organization's risk analysis due to new risks involving devices that the OCR, the Food and Drug Administration, and other government agencies have identified, such as hackers' ability to infiltrate hospital systems through medical devices.
- Update your risk management plan if necessary. Do you need new policies and procedures to address newly identified risks and vulnerabilities associated with mobile and medical devices?
- Keep your workforce members who access ePHI current with their HIPAA training requirements.

Bottom line: The OCR is clearly looking for providers to be compliant with all of these requirements.

Note: To read the OCR's Resolution Agreement and CAP with Lahey, go to www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/Lahey.html. The OCR's Resolution Agreement and CAP with Triple-S is at www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/TRIPLES.html. A guidance document on how to protect and secure ePHI when using mobile devices is at www.healthit.gov/providers-professionals/yourmobile-device-and-health-information-privacy-and-security.