Codify
BY AAPC

Health Information Compliance Alert

Case Study: Take A Hard Look At Your Last Risk Analysis To Avoid Hefty Penalties

Beware: OCR is stepping up its enforcement game in wake of OIG reports.

If you're focusing only on your electronic health record or IT systems when performing a risk analysis, you're making a potentially expensive mistake. In fact, the **HHS Office for Civil Rights** (OCR) is slapping healthcare entities with huge fines for having skimpy risk assessments and poor follow-through.

Another Self-Reported Breach Leads to OCR Investigation

Background: On Dec. 14, 2015, OCR announced a settlement agreement with the **University of Washington Medicine** (UWM) that addressed charges of potential HIPAA Security Rule violations. OCR charged that UWM failed to implement policies and procedures to prevent, detect, contain, and correct security violations.

OCR began investigating UWM after receiving a breach report on Nov. 7, 2013. The breach occurred after an employee downloaded an email attachment that contained malware that compromised UWM's IT system, which then allowed an unauthorized individual access to the electronic protected health information (ePHI) of approximately 90,000 individuals.

Of the 90,000 patients' records, approximately 76,000 patients' exposed data involved a combination of patient names, medical record numbers, dates of service, and/or charges or bill balances. The rest of the patients' exposed data included names, medical record numbers, other demographics such as addresses and phone numbers, birth dates, charges or bill balances, Social Security numbers, and insurance identification or Medicare numbers.

What Went Wrong

Good news: OCR's investigation revealed that UWM did indeed have security policies requiring its affiliated entities to have up-to-date, documented system-level risk assessments and to implement safeguards in compliance with the HIPAA Security Rule. UWM is an affiliated covered entity (CE) encompassing designated healthcare components and other entities under the **University of Washington**'s control, including the **University of Washington Medical Center**, the primary teaching hospital of the **University of Washington School of Medicine**.

According to OCR, affiliated CEs like UWM "must have in place appropriate policies and processes to assure HIPAA compliance with respect to each of the entities that are part of the affiliated group."

Bad news: But despite these policies, OCR's investigation indicated that UWM failed to "ensure that all of its affiliated entities were properly conducting risk assessments and appropriately responding to the potential risks and vulnerabilities in their respective environments."

The settlement includes a significant monetary payment of $750,000, a corrective action plan (CAP), and mandated annual reports to OCR on UWM's compliance efforts, according to the announcement.

Is OCR Action a Response to OIG Report?

"Looks like we're really seeing the fruits of all that pressure on [OCR] to enforce HIPAA," says **Jim Sheldon-Dean**, founder and director of compliance services for **Lewis Creek Systems LLC** in Charlotte, VT. Sheldon-Dean refers to a recent **HHS Office of Inspector General** (OIG) report charging that OCR isn't doing enough to enforce HIPAA compliance (see "Brace Yourself for Amped-Up EHR & HIPAA Compliance Enforcement," HICA Vol. 15, No. 11, page 82).

Lesson learned: The UWM settlement is the latest case reinforcing the need for a comprehensive risk assessment. If you aren't conducting an organization-wide, thorough risk analysis, the OCR won't offer you any favorable treatment especially if you have a breach.

"All too often we see [CEs] with a limited risk analysis that focuses on a specific system, such as the electronic medical record, or that fails to provide appropriate oversight and accountability for all parts of the enterprise," OCR Director **Jocelyn Samuels** said in a recent statement. "An effective risk analysis is one that is comprehensive in scope and is conducted across the organization to sufficiently address the risks and vulnerabilities to patient data."

Don't Hyper-Focus Your Risk Analyses

But the lesson of the UWM settlement isn't limited to organizations operating as affiliated CEs, according to a Dec. 15 analysis by Ohio-based partner **Chris Bennington** of **Bricker & Eckler Attorneys at Law**. All CEs and business associates (BAs) "should review their most recent risk analysis to determine whether it was truly comprehensive in scope."

Ask yourself: Was your most recent risk analysis limited to your EMR and other key systems, or did it include all of your organization's systems that could potentially put patient data at risk?

"In the UWM case, the organization's email system permitted a message containing malware to reach an employee's inbox, and there was apparently no other system in place to prevent the malicious attachment from opening and compromising the system," Bennington pointed out. "If UWM had conducted a more thorough risk analysis and implemented additional security on its systems, the breach and the resulting settlement may have been avoided."

Link: To read the UWM Resolution Agreement and CAP, go to www.hhs.gov/sites/default/files/uw-ra-and-cap.pdf.