SANDBERG PHOENIX

LONG TERM CARE & SENIOR LIVING BLOG

Another $750,000 HIPAA Settlement - Focus on Need for Risk Analysis

AUTHOR: SANDBERG PHOENIX

The HIPAA Final Rule has been in effect since 2013, but HIPAA settlements following breaches continue to be reported. If you think the need for a risk analysis under HIPAA is not important, think again! On December 14, 2015, the Department of Health and Human Services (HHS) announced another $750,000 HIPAA settlement with the University of Washington Medicine (UWM). This settlement not only involves a payment of $750,000 but also requires a corrective action plan and annual reports to the Office for Civil Rights (OCR) on UWM's compliance efforts. The settlement follows an OCR investigation after UWM reported a breach of electronic protected health information (ePHI) involving approximately 90,000 individuals after an employee downloaded an email attachment containing malicious malware. As a result, UWM's IT system involving 76,000 patients names, medical record numbers, dates of service, and/or charges or bill balances as well as approximately 15,000 patients' names, medical record numbers, and other demographics were compromised.

The OCR investigation revealed that UWM's security policies required affiliated entities to have up to date documented system-level risk assessment and to implement safeguards complying with the Security rule. UWM was an affiliated covered entity of the University of Washington. While there was a security policy in place, UWM failed to ensure that affiliated entities were complying with that security policy by properly conducting risk assessments and responding to the potential risks and vulnerabilities identified in their environments. OCR Jocelyn Samuels responded to this breach stating, "[a]ll too often we see covered entities 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. 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."

Lesson to be learned from UWM's settlement: Covered entities not only need to have security policies including risk assessment requirements, but must follow their policies to ensure that risks and vulnerabilities are identified to protect their environments. Covered entities take heed, the OCR takes policies such as risk assessment seriously as this UWM settlement demonstrates. Covered entities put security policies including security risk assessment in place, and follow those policies to avoid the kind of settlement UWM just entered. UWM learned, but now UWM will not only need to implement corrective action but will continue to report its compliance to the OCR in addition to a paying hefty fine. HIPAA is serious business, proactive action, including HIPAA policies that are followed, is the best defense.

By Denise Bloch

Denise Bloch

Image not found or type unknown