Oregon Health & Science hit with a $2.7 Million HIPAA settlement

Rick L. Hindmand | Tuesday, July 19, 2016

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) yesterday **announced a $2.7 million HIPAA settlement** with a large academic health center and research university, Oregon Health & Science (OHSU), which also agreed to implement a comprehensive corrective action plan.

This settlement is noteworthy as a reminder of common OCR enforcement themes revolving around risk analysis and risk management for electronic protected health information (ePHI), as well as the need for business associate agreements and encryption.

- Even though OHSU regularly performed risk analysis (six times in 10 years), OCR determined that OHSU's risk analysis process fell short by failing to cover all ePHI in OHSU's academic health center and research university, which included two hospitals and multiple clinics throughout Oregon. Furthermore, OHSU failed to implement timely measures to address the risks and vulnerabilities that were documented in the risk analysis process.

- For the fourth time in the last eight months, OCR has come down hard on a covered entity for allowing business associates to access PHI without entering into a business associate agreement. In this case, OHSU failed to obtain a business associate agreement with an internet-based service provider prior to storing ePHI on a cloud-based server. Those earlier settlements involved payments of $750,000 (**Raleigh Orthopaedic Clinic, P.A.**), $1.55 million (**North Memorial Health Care**) and $3.5 million (**Triple-S**

Management Corporation).

- OCR once again emphasized the importance of encryption as a safeguard, faulting OHSU for its failure to implement a process to encrypt and decrypt ePHI, or an equivalent alternative measure, after identifying lack of encryption as a risk.

OCR Director Jocelyn Samuels warned senior executives and board members that "[t]his settlement underscores the importance of leadership engagement and why it is so critical for the C-suite to take HIPAA compliance seriously." Risk analysis not only needs to be performed, but also must account for all ePHI within the organization. In addition, the covered entity or business associate must implement adequate safeguards to reduce the identified risks and vulnerabilities to reasonable and appropriate levels.

Rick L. Hindmand