HIPAA enforcement against business associates heats up with $650K settlement

Rick L. Hindmand | Friday, July 1, 2016

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) announced a $650,000 settlement with a business associate this week, proving the office is serious about taking strong enforcement action and imposing severe penalties against business associates for failure to implement safeguards as required under Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security and Breach Notification Rules.

This settlement continues OCR's expansion of its enforcement focus on business associates, following a string of three recent OCR settlements holding covered entities responsible for failing to enter into business associate agreements with their business associates:

- $750,000 - Raleigh Orthopaedic Clinic, P.A.
- $1.55 million - North Memorial Health Care
- $3.5 million - Triple-S Management Corporation

Background

The settlement was with Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS), and arose out of OCR's investigation of the theft of an unencrypted iPhone that contained electronic protected health information (ePHI) of 412 nursing home patients and was not password protected. CHCS provided management and information technology services as a business associate of six nursing homes that were subsidiaries of CHCS and reported the breaches to OCR in February 2014, as required under the Breach Notification Rule. OCR's commenced its investigation in April 2014, seven months after the HIPAA Omnibus Rule extended the HIPAA Privacy and Security Rules (and exposure to related penalties) to business associates.

OCR faulted CHCS for failure to:

- Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI (risk analysis)
- Implement appropriate security measures to reduce the risks and vulnerabilities to a reasonable and appropriate level (risk management).

OCR also found that CHCS had no policies addressing the removal of mobile devices or how to respond to a security incident.

CHCS agreed to pay $650,000 and implement a corrective action plan. This payment amount is substantial ($1,578 per affected individual) for a breach that affected only 412 individuals, but apparently could have been even higher. The HHS press release noted that the payment amount was determined after considering that CHCS provides unique and much-needed services to the elderly, developmentally disabled individuals, young adults aging out of foster care, and individuals living with HIV/AIDS.

To learn more about HIPAA compliance and keeping your business and patient information protected, contact the attorney listed below.

Rick L. Hindmand