SANDBERG PHOENIX

LONG TERM CARE & SENIOR LIVING BLOG

HIPPA's Not Just For Covered Entities - Recent Enforcement Action Extends To Business Associates

AUTHOR: SANDBERG PHOENIX

On June 29, 2016, the Office of Civil Rights (OCR) announced a Resolution Agreement it entered with Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) a business associate of six nursing homes. This Resolution Agreement included a monetary payment of $650,000 and a Corrective Action Plan (CAP). The CAP requires CHCS to conduct a risk analysis and risk management, to develop and maintain written policies and procedures as well as to train all members of the CHCS workforce with access to ePHI within 60 days of the CAP in compliance with HIPAA, and to submit annual reports and attestation of CHCS' compliance with the CAP for two years following the execution date of the Resolution Agreement.

Why is this a significant enforcement action? Because unlike prior Resolution Agreements for HIPAA breaches, this agreement was entered between the OCR and a Business Associate rather than a Covered Entity. The breach was first reported to the OCR in February 2014 by each of six nursing homes, Covered Entities with CHCS operating as their Business Associate. The breach reporting triggered an OCR investigation.

The breach involved unsecured electronic protected information (ePHI) on a Business Associate's stolen iPhone. The stolen iPhone was not encrypted or password protected. In addition, CHCS had failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality integrity, and availability of ePHI held by the business associate following the compliance date of the Security Rule for Business Associates beginning on September 23, 2013. CHCS also failed to implement appropriate security measures sufficient to reduce the risks and vulnerabilities to comply with the Security Rule. This Resolution Agreement is significant as it involved the ePHI of only 412 patients but imposed a penalty of $650,000. CHCS, the Business Associate, is a nonprofit entity. Most importantly, the OCR made a clear statement that Business Associates must implement the protections of the Security Rule.

In order for Business Associates as well as Covered Entities to avoid similar penalties, it is important that when providing mobile devices to employees the devices are password protected and encrypted to comply with HIPAA Security Rule safeguards. As the OCR begins its phase two HIPAA audits, Business Associates as well as Covered Entities need to take heed and focus on risk management concerns. Let this Resolution Agreement be a reminder that security mishaps can be costly, and Covered Entities as well as Business Associates need to develop processes and policies to avoid risk of data breaches.