THE
NATIONAL LAW REVIEW

Recent Enforcement Action Shows Business Associates Are Not Off the Hook

Friday, July 8, 2016

Article By Rebecca Frigy Romine
Erin Fleming Dunlap Lindsay R. Dailey
Polsinelli PC Polsinelli On Privacy

Communications, Media & Internet
Health Law & Managed Care
All Federal

Despite the fact that Business Associates have been directly subject to and liable under the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (HIPAA) since February 18, 2010 (the effective date of the relevant provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act), the Department of Health & Human Services, Office for Civil Rights (OCR), announced last Thursday, June 30, 2016, that it has entered into its first resolution agreement with a HIPAA Business Associate.

The resolution agreement is with Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) for potential violations of the HIPAA Security Rule and includes a monetary resolution payment of $650,000 and a corrective action plan (CAP). According to OCR's press release, CHCS provided management and information technology services to six skilled nursing facilities. At the time of the incident, CHCS was also the sole corporate parent of those facilities. In April 2014, OCR initiated an investigation after receiving separate notification from each of the six skilled nursing facilities that CHCS had experienced a breach of protected health information (PHI) when a CHCS-issued employee iPhone was stolen. Significantly, the iPhone was unencrypted and was not password protected. The PHI on the iPhone was extensive, and included social security numbers, information regarding diagnosis and treatment, medical procedures, names of family members and legal guardians, and medication information of 412 individuals. At the time of the incident, CHCS had no policies addressing the removal of mobile devices containing PHI from its facility or what to do in the event of a security incident. OCR also found that CHCS had no risk analysis or risk management plan.

In determining the settlement amount, OCR stated that it took into account that CHCS provides unique and much-needed services in the Philadelphia region to the elderly, developmentally disabled individuals, young adults aging out of foster care, and individuals living with HIV/AIDS. Under the CAP, OCR will monitor CHCS for two years to ensure CHCS remains compliant with its HIPAA obligations. Among other CAP obligations, CHCS is required to conduct an accurate and thorough risk assessment within 120 days of the effective date of the CAP and to develop written policies and procedures and provide those policies to OCR for review and approval within 150 days of the effective date of the CAP. A copy of the resolution agreement and CAP can be found on the OCR website.

There is no question Business Associates play a large role in creating, maintaining and transmitting PHI; they also play a large role in securing (or failing to secure) PHI. According to OCR's website, in 2015, eleven 500+ breaches (which are breaches affecting 500 or more individuals) were reported to OCR by Business Associates. In one case, Business Associate Medical Informatics Engineering reported that it was the target of a cyber-attack which affected over 3.9 million individuals. In 2016, ten 500+ breaches have been reported to OCR by Business Associates. Note: These numbers do not include Business Associate breaches affecting less than 500 individuals or breaches reported to Covered Entity clients, which is what Business Associates are required to do under the HIPAA regulations.

According to OCR Director Jocelyn Samuels: "Business associates must implement the protections of the HIPAA Security Rule for the electronic [PHI] they create, receive, maintain, or transmit from covered entities… This

includes an enterprise-wide risk analysis and corresponding risk management plan, which are the cornerstones of the HIPAA Security Rule." Based on the CHCS resolution agreement, the number of 500+ breaches that have been reported to OCR over the past two years by Business Associates, and the inclusion of Business

Associate in OCR's Phase II HIPAA Audits, which kicked off earlier this year and is scheduled to be completed by the end of 2016, it is only a matter of time before additional OCR investigations will result in resolution agreements with Business Associates. For those Business Associates who have not yet focused on their HIPAA compliance, the CHCS resolution agreement is yet another indicator that OCR means business.

Source URL: https://www.natlawreview.com/article/recent-enforcement-action-shows-business-associates-are-not-hook