PUBLICATION

$650,000 Lesson in HIPAA Compliance for Business Associates: Nursing Home Management Company Settles with Government

August 10, 2016

Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) settled potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule after the theft of a CHCS mobile device compromised the protected health information (PHI) of 412 nursing home residents. At the time of the breach, CHCS was the sole corporate parent to six nursing homes in the Philadelphia region for the elderly, developmentally disabled individuals, young adults aging out of foster care and individuals living with HIV/AIDS. CHCS is a nonprofit corporation providing management services, including information technology services, to nursing homes. CHCS has agreed to pay a $650,000 settlement and implement an extensive corrective action plan.

The U.S. Department of Health and Human Services Office for Civil Rights (OCR) initiated its investigation on April 17, 2014, after receiving notification that CHCS had experienced a breach of PHI involving the theft of a CHCS-issued employee smartphone. The smartphone was neither encrypted, nor password protected. The information on the smartphone was extensive and included social security numbers, information regarding diagnosis and treatment, medical procedures, names of family members and legal guardians, and medication information. At the time of the incident, CHCS reportedly 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 determined that CHCS had no risk analysis or risk management plan.

This settlement underscores the importance of maintaining a robust HIPAA compliance program for both business associates and covered entities. Although many of the compliance responsibilities for business associates and covered entities will necessarily be intertwined, entities should remain mindful of their separate and independent obligations under HIPAA. As noted by OCR, the first step in this process is for business associates and covered entities to assess whether they have a documented enterprise-wide risk analysis and corresponding risk management plan in place. To read more about the settlement, please click here.

Please contact any attorney within Baker Donelson's Privacy and Information Security Group should you have any questions or otherwise wish to discuss any of these new privacy and related initiatives.