Insights: Alerts

Largest Health & Human Services HIPAA Settlement Wake-Up Call for Covered Entities to Evaluate and Mitigate Risks

August 5, 2016

Written by **Gunjan R. Talati** and **Jon Neiditz**

On Thursday, August 4, 2016, the U.S. Department of Health & Human Services, Office of Civil Rights (OCR) announced the largest settlement ever with a single entity for multiple potential Health Insurance Portability and Accountability (HIPAA) violations. Specifically, Advocate Health Care Network, the largest health care system in Illinois, agreed to pay $5.55 million and implement a corrective action plan. The settlement stems from "the extent and duration of the alleged noncompliances…and the large number of individuals whose information was affected."

OCR started investigating Advocate in 2013 after Advocate notified OCR of three breaches. One breach involved four laptops stolen from an office building. A second breach concerned the unauthorized access of a computer network, and the third breach involved the theft of a computer from an employee's vehicle. The potentially compromised information included a variety of protected health information such as patient names, addresses, health insurance information, credit card numbers, and clinical information.

The settlement is intended to scare entities subject to HIPAA into performing "a comprehensive risk analysis and risk management to ensure that individuals' [electronic protected health information] is secure." OCR further explained that covered entities must implement "physical, technical, and administrative security measures sufficient to reduce the risks to ePHI in all physical locations and on all portable devices to a reasonable and appropriate level."

This settlement should serve as a wake-up call to all covered entities subject to HIPAA to assess and mitigate their risks by:

-- Evaluating risks and vulnerabilities of protected health information and establishing internal controls that address those risks and vulnerabilities;
-- Implementing controls that limit access to information systems with protected health information (including encryption meeting HIPAA breach rule standards for computers and mobile devices);
-- Ensuring business associates understand their obligations to safeguard protected health information; and
-- Implementing safeguards for transmitting and transporting protected health information.

By performing these housekeeping measures, entities handling protected health information may prevent or mitigate HIPAA violations. OCR's settlement with Advocate sends a clear message that failing to comply could be an expensive proposition. And although HHS still limits its enforcement of breaches, the FTC has made it clear in *LabMD* that it will pursue the same covered entities and business associates for mere vulnerabilities in the absence of a breach.

For additional information or assistance in conducting a risk assessment, please contact one of the authors or your regular Kilpatrick Townsend contact.

Related People

Gunjan R. Talati

t 404.815.6503

gtalati@ktslaw.com

Jon Neiditz

t 404.815.6004

jneiditz@ktslaw.com