MURTHA CULLINA

NEWS ALERT

HEALTH CARE

Providers Beware: OCR Published Three HIPAA Settlements in Two Weeks, Signaling a Ramp Up of HIPAA Enforcement Activity:

Make sure risk assessments, business associate agreements and policies & procedures are in place and up to date

By Stephanie S. Sobkowiak and Daniel J. Kagan | April 25, 2017

In a two week period, the United States Department of Health and Human Services, Office for Civil Rights (OCR) published settlements with three different health care providers for violations of HIPAA. The settlements were not insignificant, ranging from $31,000 for a small physician practice, to $400,000 for a federally qualified health center (FQHC), to $2,500,000 for a wireless health services provider. Each of these violations and subsequent settlements should act as a cautionary tale to providers, both large and small, that they must continue to be vigilant in their HIPAA compliance efforts.

On April 12, OCR reached a $400,000 settlement, resolution and corrective action plan with an FQHC. In late January 2012, the FQHC experienced a breach due to a phishing incident. While the FQHC took corrective action to prevent similar events from occurring in the future, OCR's subsequent investigation exposed that the FQHC failed to conduct its first risk analysis until mid-February 2012, weeks after the incident. Further, OCR deemed that this first risk analysis, and all subsequent risk analyses performed by the FQHC, were insufficient to meet the HIPAA Security Rule requirements.

On April 20, OCR reached a $31,000 settlement, resolution and corrective action plan with a small pediatric subspecialty practice. The practice used a business associate to store records containing protected health information (PHI). After a compliance review, OCR investigated the practice and discovered that it did not have a signed business associate agreement in place with the records storage company until approximately twelve years after it started using the company.

On April 24, OCR reached a $2,500,000 settlement, resolution and corrective action plan with a company that provides remote mobile monitoring of, and rapid response to, patients at risk for cardiac arrhythmias. This settlement represents the first in which OCR focused on a wireless health services provider. The company experienced a breach when an employee's laptop, containing PHI of nearly 1,400 patients, was stolen from his car, parked outside his home. After the company reported the breach to OCR, OCR conducted an investigation. This investigation uncovered that the company: (1) conducted an insufficient risk analysis and had an inadequate risk management process; (2) had only draft policies and procedures to implement the HIPAA Security Rule; and (3) had no final policies or procedures implementing safeguards for electronic PHI, including those for mobile devices containing PHI.

These enforcement actions should serve as reminders to providers of all types and sizes, as we predict that OCR's enforcement actions will continue. If you have any questions regarding these settlements, HIPAA or health law in general, please contact Stephanie, Daniel, Dena or another member of our Health Law Practice Group.

Stephanie S. Sobkowiak at 203.772.7782 or ssobkowiak@murthalaw.com
Daniel J. Kagan at 203.772.7726 or dkagan@murthalaw.com
Dena M. Castricone at 203.772.7767 or dcastricone@murthalaw.com