MURTHA CULLINA

NEWS ALERT

HEALTH CARE

A HIPAA Compliance Program "In Disarray" Leads to OCR Imposing a $2.15 Million Civil Monetary Penalty

By Daniel J. Kagan | October 30, 2019

Last week, the U.S. Department of Health and Human Services Office for Civil Rights ("OCR") imposed a civil monetary penalty ("CMP"), to the tune of $2.15 million, against Jackson Health System ("JHS"). The CMP stemmed from JHS' numerous HIPAA violations that occurred from 2013 through 2016.

JHS' HIPAA violations ran the gamut, from lost paper records, to impermissible media disclosures, to violations of the minimum necessary rule, to a rogue employee selling patients' protected health information ("PHI"). OCR's Director, Roger Severino, noted that JHS' "HIPAA compliance program . . . had been in disarray for a number of years."

With regard to the lost paper records, in August 2013, JHS submitted a breach report to OCR, notifying OCR that it lost paper records that contained the protected health information ("PHI") of over 700 patients. However, subsequent to making the report, upon its own internal investigation, JHS discovered that it had lost three additional boxes of paper records in December 2012. JHS did not report this loss to OCR until June 2016, even though this breach doubled the number of affected patients.

In June 2015, OCR initiated an investigation against JHS after it discovered that a reporter shared a photo of a JHS operating room screen that contained a patient's PHI. After this publication, JHS discovered that two of its employees violated the minimum-necessary rule, accessing this patient's record without having a job-related purpose.

In February 2016, JHS experienced the most egregious of its HIPAA violations. JHS submitted a breach report to OCR indicating that a JHS employee inappropriately accessed over 24,000 patient records and had been selling patients' PHI.

Through OCR's investigation of the above incidents, it uncovered that JHS failed to provide timely breach response, did not conduct enterprise-wide risk analyses, did not perform audits of system activity, and did not have any restrictions in place to prevent workforce members' access to patients' electronic PHI.

There are some important takeaways from this latest OCR enforcement action. First, covered entities and business associates, both large and small, should take time to conduct an overall assessment of their HIPAA compliance programs. Second, organizations should ensure that they audit employee access, focusing on those records where there is not likely to be a job-related purpose (*e.g.* persons in the media, co-workers, family members). Third, covered entities should implement reasonable restrictions to prevent classes of workforce members from impermissibly accessing PHI. Lastly, covered entities should take care when interacting with the media, to ensure that there are no inadvertent disclosures of PHI without a proper HIPAA authorization from the patient.

If you have any questions or need assistance with policy and procedure drafting or review, please contact Stephanie S. Sobkowiak at 203.772.7782 or ssobkowiak@murthalaw.com or Daniel J. Kagan, at 203.772.7726 or dkagan@murthalaw.com.

Paul E. Knag, Co-Chair
203.653.5407
pknag@murthalaw.com

Stephanie S. Sobkowiak, Co-Chair
203.772.7782
ssobkowiak@murthalaw.com

Heather O. Berchem
203.772.7728
hberchem@murthalaw.com

Julia P. Boisvert
860.240.6018
jboisvert@murthalaw.com

Daniel J. Kagan
203.772.7726
dkagan@murthalaw.com

Madiha M. Malik
203.772.7710
mmalik@murthalaw.com

Mindy S. Tompkins
860.240.6063
mtompkins@murthalaw.com