MURTHA CULLINA
ATTORNEYS AT LAW

NEWS ALERT

HEALTH CARE

A Reminder That Covered Entities Of All Sizes Need To Comply With HIPAA Security Rule

By Daniel J. Kagan | March 4, 2020

On March 3, 2020, the U.S. Department of Health and Human Services Office for Civil Rights ("OCR") signaled to covered entities of all sizes that they need to take their HIPAA obligations seriously. OCR entered into a settlement and corrective action plan with a small physician practice for $100,000 to settle alleged violations of the HIPAA Security Rule. This enforcement action is an example of OCR enforcing HIPAA's requirements on smaller covered entities. OCR specifically noted that this practice sees approximately 3,000 patients per year.

This settlement occurred following OCR's investigation of the practice after it filed a breach report related to a dispute with a business associate. During the investigation, OCR uncovered that the practice never conducted a risk analysis at the time of the breach report and, despite receiving significant technical assistance during the investigation, the practice failed to complete a thorough risk analysis after the breach. Risk analyses are critical for covered entities to identify risks and vulnerabilities and to address them at an appropriate level. OCR's Director, Roger Severino summed it up by stating: "The failure to implement basic HIPAA requirements, such as an accurate and thorough risk analysis and risk management plan, continues to be an unacceptable and disturbing trend within the health care industry."

Conducting a risk analysis is a foundational step that covered entities must take to understand their vulnerabilities and, even more importantly, to understand where they should implement safeguards to best protect the electronic health information they maintain. While there is no one-size-fits-all method for conducting a risk analysis, as HIPAA is scalable based on the size and complexity of the covered entity, this enforcement action shows that small providers need to take this responsibility seriously. It is important to note that the risk analysis process should be an ongoing process. HIPAA does not prescribe how often a covered entity needs to conduct a risk analysis; however, given a shifting technological environment, best practice would be to conduct these analyses every two to three years or sooner when implementing new technology (*e.g.* moving to a cloud-based server or moving to a new electronic health record vendor).

If you have any questions about conducting a risk analysis or any other HIPAA questions, 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