OCR to Increase Investigations Of Smaller PHI Breaches

Articles, Privacy, Technology and Data Security August 29, 2016

Healthcare providers and other covered entities[1] must report breaches of unsecured protected health information ("PHI") to the Secretary of Health and Human Services in accordance with the Breach Notification Rule of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Each breach involving more than 500 individuals is investigated by the Office for Civil Rights ("OCR") to assess the root cause of the breach and address any instances of HIPAA noncompliance within the covered entity.

Over the last couple of years, we have seen OCR start investigating more and more smaller breaches. Theft of PHI is one factor that has played a role in whether or not smaller breaches are investigated.

The first breach involving less than 500 individuals that OCR investigated concerned the Hospice of North Idaho ("HONI"). In this case, an unencrypted laptop containing PHI of 441 patients was stolen. OCR found that HONI had not conducted a risk analysis or implemented any policies or procedures to safeguard PHI stored on mobile devices. More recently, Catholic Health Care Services of the Archdioceses of Philadelphia (CHCS) agreed to settle potential violations of the HIPAA Security Rule for $650,000. In this case, PHI of 412 nursing home residents was compromised due to the theft of a CHCS-issued employee mobile device. The mobile device was not encrypted or password protected and contained highly sensitive information including social security numbers, medical diagnosis, and treatments. CHCS did not have any policies in place related to the use of mobile devices offsite. CHCS also failed to show that they had performed a risk assessment or implemented a risk management plan, which OCR views as "cornerstones of the HIPAA Security Rule."

Recently, OCR announced new initiatives that will increase investigations of smaller breaches involving less than 500 individuals. Theft of unencrypted PHI continues to be one factor that OCR will consider when determining whether or not to conduct an investigation. Other factors include the size of the breach, the nature of the PHI involved, whether the breach involved any unwanted intrusions to IT systems, and whether there are numerous breach reports from the same covered entity or business associate.

The increased scrutiny OCR will give to smaller breaches highlights the importance for all covered entities to address security issues related to mobile devices. All mobile devices must be properly encrypted and steps must be taken to reduce the risk of theft as much as possible. In addition, covered entities must perform risk assessments and implement risk management plans and other policies regarding mobile device security. A failure to do so could result in the covered entity paying hundreds of thousands of dollars to settle investigations with OCR.

If you would like more information on implementing new mobile device policies, or an audit of your existing policies, contact Kristin Biedinger

[1] "Covered Entity" is defined as: (1) a health plan; (2) a health care clearinghouse; or (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter [e.g., HIPAA Administrative Simplification transaction standards]. (45 CFR §160.103).