SANDBERG PHOENIX

PHYSICIAN LAW BLOG

HIPAA News - $750,000 Settlement Following Stolen Laptop

AUTHOR: DIANE ROBBEN

Ever wonder if the Office of Civil Rights ("OCR") is serious about the requirements for a HIPAA Security risk analysis and policy specific to removing hardware and electronic media containing ePHI from a covered entity's facility? Yes, the OCR is extremely serious about those requirements as Cancer Care Group, P.C. ("Cancer Care"), a radiation oncology private practice, with 13 radiation oncologists discovered after reporting a breach of ePHI.

The OCR announced that Cancer Care entered a $750,000 settlement with the OCR as a result of a breach involving ePHI for approximately 55,000 Cancer Care patients following the theft of a laptop bag from an employee's car. The laptop bag included the employee's laptop and unencrypted backup media, which contained names, addresses, dates of birth, Social Security numbers, insurance information and clinical information of about 55,000 current and former Cancer Care Group patients.

After Cancer Care reported the breach to the OCR as required by HIPAA, the OCR conducted an investigation. The OCR discovered two significant problems, either of which may have reduced the likelihood of the breach. First, Cancer Care had failed to conduct an enterprise-wide risk analysis prior to the breach, which occurred in July 2012. Second, Cancer Care did not have a written policy specific to removing hardware and electronic media containing ePHI into and out of its facilities, even though it was common practice within the organization to do so. The OCR found that had Cancer Care performed a security risk assessment, it would have identified that removing unencrypted back media was an area of significant risk to Cancer Care's ephi. In addition, if there had been a comprehensive device and media control policy, it could have provided direction to employees as to their responsibilities to protect such devices when removing them from the facility. Finally, while encryption is not required by HIPAA, if Cancer Care had proper encryption of its mobile devices and electronic media it would have reduced the likelihood of a breach of protected health information.

You may ask why does a security risk analysis and policy for removing hardware and electronic media containing ePHI matter? In addition to the $750,000 settlement imposed on a small group of 13 physicians, Cancer Care also was required to take corrective action to meet the specific requirements of HIPAA and entered a Corrective Action Plan. In addition to the requirements for corrective action, Cancer Care is required to submit annual reports for three years to demonstrate HIPAA compliance to the OCR.