$4.3 Million HIPAA Penalty for Breach of Unencrypted PHI

A U.S. Department of Health and Human Services (HHS) administrative law judge (ALJ) ruled that a cancer treatment center violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The violation occurred when the electronic protected health information (ePHI) of more than 33,000 individuals was breached after an unencrypted laptop computer was stolen from a teleworker’s home and two other workers from the cancer treatment center lost unencrypted USB drives. The result of the HIPAA violation requires the cancer treatment center to pay a penalty of more than $4.3 million.

The HHS Office for Civil Rights (OCR) conducted an investigation after three separate data breach reports in 2012 and 2013. The investigation resulted in a finding that the cancer treatment center, dating back to 2006, had recognized the need to encrypt devices to address a high risk to ePHI. The center had written encryption policies to address the risks but failed to adopt enterprise-wide encryption until 2011. Even then, it did not fully implement its encryption policy until 2013. OCR proposed penalties of $2,000 per day from March 2011 to January 2013 for the failure to encrypt and penalties of $1.5 million per year for 2012 and 2013 for the unauthorized disclosures of ePHI. The cancer treatment center opposed OCR allegations and determinations of regulatory violations.

The cancer treatment center argued that it was not obligated to encrypt its devices and that the ePHI at issue here was for research and therefore was not subject to HIPAA nondisclosure requirements. Finally, the cancer treatment center argued that the penalties imposed are unreasonable. The ALJ rejected all of these arguments, citing the high risk to patients of unauthorized disclosure of ePHI and the delay in implementing encryption procedures despite the recognized need for enterprise-wide encryption. The ALJ reiterated that there is nothing in the HIPAA regulations that provides an exemption for information or data that is used in research, particularly where there is patient data that reveals their names, Social Security numbers, medical diagnoses and treatments. While there may be limited exemptions for research conducted by noncovered entities, that is not the case here, and the disclosure of ePHI by the cancer treatment center as a covered entity is clearly subject to HIPAA.