Judge upholds fourth largest HIPAA penalty of $4.3 million for Texas cancer center

June 22, 2018

The U.S. Department of Health and Human Services Office of Civil Rights (OCR) announced that an administrative law judge has upheld its fourth largest HIPAA penalty against the University of Texas MD Anderson Cancer Center. MD Anderson, an academic institution and cancer treatment and research center based in Houston, Texas, has been ordered to pay $4.3 million in civil monetary penalties to resolve HIPAA violations that arose from three data breaches that occurred in 2012 and 2013.

During that period, an MD Anderson employee's laptop was stolen from his residence, an intern lost a USB thumb drive and a visiting researcher lost an additional USB thumb drive. The devices, which contained the electronic protected health information (ePHI) of 34,883 patients, were not password protected or encrypted.

OCR's investigation into the breaches revealed that MD Anderson had developed policies requiring portable devices like laptops and USB thumb drives to be encrypted as far back as 2006. However, OCR found that the cancer center did not begin implementing encryption until 2011 and had not encrypted all of its portable electronic devices until 2013. MD Anderson's prior risk analyses and annual reports identified this lack of encryption for portable devices as a high-risk area to the security of ePHI.

MD Anderson disagreed with OCR's penalty based on its argument that the ePHI at issue was used for research purposes and that the research was not subject to HIPAA's encryption or disclosure requirements. Additionally, MD Anderson contested the assessed penalty on the basis that it was unreasonable.

The administrative law judge reviewing the penalty found that MD Anderson had "consistently failed to implement the very

measures it had identified as being necessary to protect that information" and upheld the penalties. Leaders for MD Anderson have stated that they plan to appeal the decision.

Authors