# Health Information Compliance Alert

## Case Study: Follow Through on Your Risk Issues or Pay the Price

**Encryption fails bring massive penalties, OCR case shows**

The HIPAA Security Rule requires covered entities (CEs) to assess, analyze, and manage practice risks to safeguard patient and provider data. Taking a lax approach to these federally-mandated security policies and procedures - especially risk assessments and the management of observed threats - only leads to disaster. Unfortunately, one organization learned this truth the hard way.

**Background:** Back in 2012 and 2013, the HHS Office for Civil Rights (OCR) looked into three separate breaches at University of Texas MD Anderson Cancer Center (MD Anderson). The incidents involved "the theft of an unencrypted laptop from the residence of an MD Anderson employee and the loss of two unencrypted universal serial bus (USB) thumb drives containing the unencrypted electronic protected health information (ePHI) of over 33,500 individuals," said an OCR release.

**Big deal:** In the midst of the investigation, the agency discovered that MD Anderson ignored encryption policy suggestions dating to 2006, despite risk analyses that uncovered dangers to ePHI, the report indicated. The kicker in this case, however, was the organization slow walking its encryption policy installations. "MD Anderson did not begin to adopt an enterprise-wide solution to implement encryption of ePHI until 2011, and even then it failed to encrypt its inventory of electronic devices containing ePHI between March 24, 2011 and January 25, 2013," the OCR release stressed.

**Ponder the Consequences**

The three violations were serious infractions, but the agency gripe also surrounded MD Anderson's decision to delay encryption across its various devices for years in spite of the risk analyses' advice. This led to an eventual OCR Notice of Determination issued to the organization on March 24, 2017 with a significant fine of over $4.3 million in Civil Monetary Penalties (CMPs).

"We regularly see organizations with policies and procedures in place, but they have stopped there," explains attorney **Kathleen D. Kenney, Esq.**, of **Polsinelli LLP** in Chicago. "The implementation piece of HIPAA compliance is integral to breach avoidance."

**The saga continues:** Though MD Anderson treated patients with cancer, it also conducted research during the OCR's reviews. However, MD Anderson insisted the ePHI under investigation was for "'research' and thus was not subject to HIPAA's nondisclosure requirements," according to the release.

MD Anderson opposed the OCR's summary judgment and staunchly defended its stance that the devices holding the ePHI in question did not need to be encrypted, suggested the HHS Administrative Law Judge (ALJ) decision. The organization went on to file its own brief in opposition, the decision showed. Though arguments were made by MD Anderson that it was being unjustly punished, the facts remained: The organization did not act on its own policies.

**The final decision:** In the end, the ALJ ruled on the side of OCR and the protection of patients' ePHI, granting "summary judgment to the OCR on all issues, requiring MD Anderson to pay $4,348,000," the agency release said.

"It is easy to lose sight of what is really at issue here in the blizzard of arguments and counterarguments," said the ALJ. "This case is in its present posture because Respondent [MD Anderson] recognized a problem, consisting of the vulnerability of its ePHI to unauthorized disclosure including by loss or theft, devised a mechanism to protect ePHI that included encryption of devices, and failed to implement that mechanism."

The ALJ added, "The theft of the laptop illustrates why it was essential for Respondent [MD Anderson] to implement its

encryption policy.”

**Feds reaction:** "OCR is serious about protecting health information privacy and will pursue litigation, if necessary, to hold entities responsible for HIPAA violations,” said OCR Director **Roger Severino** in the agency release. "We are pleased that the judge upheld our imposition of penalties because it underscores the risks entities take if they fail to implement effective safeguards, such as data encryption, when required to protect sensitive patient information.”

**Resource:** To see the MD Anderson case details with links to both the Notice of Determination and the ALJ's ruling, visit www.hhs.gov/about/news/2018/06/18/judge-rules-in-favor-of-ocr-and-requires-texas-cancer-center-to-pay-4.3-million-in-penalties-for-hipaa-violations.html.