NOW + NEXT

HIPAA ALERT | NIXON PEABODY LLP

JUNE 26, 2018

Judge affirms OCR's fourth-largest judgment for HIPAA violations

By Valerie Breslin Montague, Laurie Cohen, and Christopher Tonellato

On June 1, 2018, a Department of Health and Human Services (HHS) Administrative Law Judge ("ALJ") granted a summary judgment motion in favor of Office for Civil Rights (OCR) upholding the fourth-largest judgment for HIPAA violations. $4,348,000 of civil money penalties were imposed on The University of Texas MD Anderson Cancer Center ("MD Anderson"). By challenging the OCR fine and proceeding before the ALJ, MD Anderson avoids a resolution agreement with OCR and the imposition of a corrective action plan.

The OCR investigation into MD Anderson, and its subsequent 2017 Notice of Proposed Determination, stemmed from breaches of patient information resulting from the theft of an unencrypted laptop and the loss of two unencrypted USB drives. These devices contained patient names, social security and medical record numbers and diagnoses for 34,883 individuals. OCR argued and the ALJ found that MD Anderson was in noncompliance with two HIPAA regulations regarding the protection of electronic protected health information ("ePHI"). The first requires entities covered by HIPAA to protect electronic information systems from unauthorized disclosures of ePHI. The second prohibits a covered entity from disclosing ePHI unless otherwise permitted in the regulations.

The ALJ found that, as early as 2006, MD Anderson had written policies requiring encryption or access controls on mobile devices, such as laptops, which contained ePHI. He also found that MD Anderson identified mobile media security as a high-level risk in 2007. However, the ALJ stated that MD Anderson made only "half-hearted and incomplete efforts at encryption," finding that it did not implement its policies on an enterprise-wide basis until May 2012. Although the hospital argued that it was not required by HIPAA to implement encryption, the decision serves as a reminder to HIPAA-regulated entities that the addressable standards in the HIPAA regulations, such as encryption, are not "optional." If an entity chooses not to implement addressable standards, the HIPAA Security Rule requires that the entity document why it is not feasible to do so and implement an alternative measure. OCR, in its 2017 Notice of Proposed Determination, describes how MD Anderson did not document the reasons why encryption was not feasible and, for a period of more than two years, did not implement an equivalent alternative measure.

The ALJ acknowledged the hospital's argument that the HIPAA regulations do not require encryption but agreed with OCR that MD Anderson did not implement an equivalent alternative. The ALJ stated that encryption was the mechanism that MD Anderson chose to protect its ePHI. Once MD Anderson chose encryption as its means of safeguarding ePHI, the ALJ determined that it was obligated to implement this policy and encrypt its mobile devices. A key take-away from this decision is that if a covered entity or business associate identifies risks in its HIPAA security risk assessment process, it is imperative that the entity eliminate, mitigate or otherwise manage that risk through the entity's risk management plan. Further, the entity should ensure that its risk management plan is implemented on an enterprise-wide basis.

OCR found that the length of time that the hospital continued to use unencrypted devices after determining that encryption was necessary was an aggravating factor in determining the penalty amount.

MD Anderson expressed its intent to appeal the ALJ ruling. A copy of the decision may be found here.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

— Valerie Breslin Montague, 312-977-4485, **vbmontague@nixonpeabody.com**

— Laurie T. Cohen, 518-427-2708, **lauriecohen@nixonpeabody.com**