

Report on Patient Privacy Volume 18, Number 7. July 31, 2018 Lack of Encryption Key to \$4.3M Penalty For MD Anderson; 'Layered Security' One Solution

By HCCA Staff

The \$4.3 million penalty slapped on MD Anderson Cancer Center for allegedly violating the HIPAA regulations will stand, at least for now. Administrative Law Judge (ALJ) Steven Kessel sided with the HHS Office for Civil Rights (OCR), which fined the Houston health system last year in connection with three breaches that led to the disclosure of 33,500 people's electronic protected health information (ePHI) when an unencrypted laptop and two thumb drives went missing.

MD Anderson appealed, arguing the fines were unreasonable, that it wasn't required to encrypt the ePHI, and that the information isn't subject to HIPAA nondisclosure requirements because it's research related.

But the ALJ wasn't buying.

"The penalties in this case are reasonable given the gravity of Respondent's noncompliance and the number of individuals potentially affected," Kessel said in the decision (No. CR51110). "What is most striking about this case is that Respondent knew for more than five years that its patients' ePHI was vulnerable to loss and theft and yet, it consistently failed to implement the very measures that it had identified as being necessary to protect that information."

The tug of war isn't over, however. MD Anderson said it will appeal. "We hope this process brings transparency, accountability and consistency to the Office for Civil Rights' enforcement process," according to a statement.

A lot of HIPAA penalties hit organizations that fall short on HIPAA security risk assessments, but this time it's also about the alleged failure to follow through, says attorney Richelle Marting, with the Forbes Law Group in Overland Park, Kansas. "It's not just the thought that counts. You have to do something with your security risk assessment or you will face penalties."

This document is only available to subscribers. Please [log in](#) or [purchase access](#).

[Purchase Login](#)