Report on Patient Privacy Volume 18, Number 8. August 31, 2018 MD Anderson Cancer Center's Travails Show Struggle to Encrypt, OCR 'Impatience'

By HCCA Staff

So far this year, the HHS Office for Civil Rights (OCR) has announced financial penalties with just two covered entities (CEs) and one business associate (BA) accused of HIPAA violations. For the CEs, the penalties were in the millions, while the BA got off comparatively easily with just $100,000.

In contrast to 2017, the pace of OCR's enforcement has slowed: by this time last year, the agency had announced nine of the 10 cases it would resolve by the start of 2018.

But what OCR may lack in volume, it has somewhat made up in intrigue, particularly with its most recent enforcement action. In June, OCR announced that an administrative law judge (ALJ) had sided with the agency and was imposing a $4.358 million penalty on the University of Texas MD Anderson Cancer Center for HIPAA violations (*RPP 7/18, p. 1*). MD Anderson has said it plans to appeal.

OCR always recommends that CEs and BAs examine settlements and other enforcement actions for lessons they can glean to keep them out of similar trouble. MD Anderson's situation is especially compelling for a variety of reasons, including the continuation of the case beyond the point where most are resolved.

To help with an analysis of the MD Anderson situation, *RPP* consulted with Marti Arvin, vice president of audit strategies for the security consulting firm CynergisTek Inc. Arvin's previous positions include chief compliance officer for the University of California Los Angeles Health and chief privacy officer for the University of Louisville.

MD Anderson's $4.358 million penalty is the fourth biggest in OCR's history and follows the agency's pattern of increasingly high penalties for what may be relatively small numbers of affected patients. MD Anderson's lost devices at issue contained protected health information (PHI) for 33,500 individuals. OCR also found fault with MD Anderson's encryption program—citing the fact that it had, as of January 2013, "reported to OCR that it had encrypted 98% of its total managed computer inventory (33,385 computers)."

For comparison, OCR's largest settlement was for $5.55 million with Advocate Health Care of Illinois. The breach that triggered that settlement began with the theft of desktop computers that contained the PHI of 4 million patients (*RPP 9/16, p. 1*).

The two previous settlements this year were both announced in February. OCR opened the year with a $3.5 million settlement with Fresenius Medical Care North America, which also agreed to a two-year corrective action plan (CAP).