COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 19, Number 5. May 08, 2019 Should 'State' Agencies Be Exempt From HIPAA? MD Anderson Says Yes

By Theresa Defino

After failing to convince HHS administrative law judges (ALJs) that research data doesn't have to be protected under HIPAA, the University of Texas MD Anderson Cancer Center has filed its third appeal to try to keep from paying $4.358 million for breaches in 2012 and 2013 that collectively exposed information about approximately 35,000 individuals.

In early April, MD Anderson filed suit against HHS Secretary Alex Azar in the U.S. District Court for the Southern District of Texas; this time it is arguing that the Office for Civil Rights (OCR) lacks the authority under HIPAA to fine MD Anderson because it is a type of state agency and that the fines imposed are excessive. Both arguments were also advanced at the ALJ level, but those judges said they did not have the jurisdiction to address them.

HHS has not yet filed its response. But to its argument that OCR exceeded allowable fines, MD Anderson seems already to have won. Just a few weeks after its suit was filed, OCR announced it would no longer apply an across-the-board annual maximum of $1.5 million, regardless of the severity of the violation. If the new fines are applied to MD Anderson, it would signal a big win for it.

Appeals Unsuccessful to Date

Typically, OCR is able to reach settlement agreements with organizations it believes have violated the privacy, security or breach notification regulations under HIPAA. OCR tried from October 2015 to August 2016 to do so, but MD Anderson refused, and in March 2017, OCR ended negotiations and moved to collect payment. MD Anderson then appealed to an ALJ, making the research argument, contending also that the data had not come to any harm or misuse, and that encryption was an "optional standard." It raised other arguments, mounting what ALJ Judge Steven T. Kessel termed a "blizzard of arguments and counter-arguments."

In July, OCR announced that Kessel had upheld its decision to fine MD Anderson $1.5 million for a stolen laptop and a USB drive lost in 2012 and $1.5 million for another drive reported missing in 2013. It added another $1.348 million for failing to implement access controls, specifically encryption and decryption ("Lack of Encryption Key to $4.3M Penalty For MD Anderson; 'Layered Security' One Solution," *RPP* 18, no. 7).

At the time, MD Anderson said it was disappointed by the ruling and planned to launch a further appeal. In February, a three-member Department of Appeals Board upheld Kessel's opinion. In a 33-page ruling, the judges dismissed MD Anderson's claim that the security regulation does not require encryption, stating that it had planned to implement encryption but simply had delayed doing so due to financial concerns. The trio also batted back MD Anderson's continued assertion that research data is not covered under HIPAA, relying on language in the preamble of the privacy rule as published in 2000. The appeals board said MD Anderson offered no new information to support this argument.

On April 9, MD Anderson filed a 15-page appeal in the Texas district court.

In the appeal, MD Anderson seems to be arguing that penalty amounts are also inappropriate because the

“alleged disclosure violations” were out of character for the rest of the workforce, noting that they were caused by “three MD Anderson employees out of more than 21,000 over a 2-year period.”

In contrast to the earlier pleadings, it did not raise the issue of research data being exempt, but focused instead on two other arguments: that MD Anderson itself is exempt from civil monetary penalties, which it deemed inappropriately high. And it continued to dispute that it was not in compliance regarding encryption, which it defined as “optional.”

It took issue with the $2,000-per-day fine for failing to encrypt from March 24, 2011, to Jan. 25, 2013, based on a “reasonable cause” category of fines. “MD Anderson had appropriate policies in place and pursued encryption efforts in light of available technologies and considerations for uninterrupted, critical patient care,” it said in the appeal.

MD Anderson said the $3 million for the 2012 and 2013 losses of electronic protected health information equated to “the maximum amount that the OCR could impose under any level of culpability under HIPAA, making the punishment the same as in a case in which ePHI was intentionally taken to cause harm to patients and where harm was actually incurred.” The cancer center said the fines were in violation of annual caps imposed per identical violation.

Given OCR’s recent reduction in annual caps, the agency appears to agree.