COSMOS
Navigate the Compliance Universe

Report on Research Compliance Volume 16, Number 5. May 01, 2019 MD Anderson Appeals $4.38 Million Imposed For HIPAA Breaches, Argues Exempt Status

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.

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 ("MD Anderson Held to $4.3 Million for HIPAA Violations; Research Data Ruled Not Exempt," *RRC* 15, no. 8.)

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.

Stongest Argument for Exemption?

According to the appeal, OCR "claimed authority" to issue the civil monetary penalty under HIPAA, but that the statue says such fines can only be imposed on a "person," defined as "a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private." Fining MD Anderson represents an expansion of the statute to unlawfully apply to "states and state agencies," the suit alleges.

Should the court side with MD Anderson on this point, "that would mean that any organization that is a part of the state entity—a health care organization or a state health plan or potentially state Medicaid plans—is not a person under HIPAA," Marti Arvin, a consultant specializing in HIPAA and research, told *RRC*.

This could mean a "significant number of organizations that [potentially] could say they're not under the purview of the HIPAA regulations," said Arvin, executive advisor for CynergisTek Inc.

Arvin predicted, however, that "if the court can find a way to say that OCR had the authority to revise the definition in this way to meet congressional intent, I think they will. Because I think [otherwise] it just opens up a huge can of worms." Still, she said this argument may have a greater chance of success than the others in MD Anderson's appeal.

MD Anderson did not answer any questions from *RRC*, but issued the following statement on the appeal: "Patient privacy is of extreme importance at The University of Texas MD Anderson Cancer Center, and substantial measures are in place to ensure the protection of patient information. Throughout this legal process, MD Anderson has committed to bringing this matter to federal court given its status as a state institution and the failure of the administrative judges to consider all of MD Anderson's legal arguments. Additionally, given the circumstances of the incidents, we believe the penalties are inappropriate and excessive. Regardless of the final decision, MD Anderson hopes this process brings transparency, accountability and consistency to the Office for Civil Rights' enforcement process. The institution remains committed to safely protecting patient information."