COSMOS
Navigate the Compliance Universe

Report on Research Compliance Volume 15, Number 10. October 31, 2018
To Foster HIPAA Compliance, Focus On Risks Inherent in Research Settings

By Theresa Defino

In June, the HHS Office for Civil Rights (OCR) announced that a judge had upheld a $4.3 million fine against the University of Texas MD Anderson Cancer Center for HIPAA violations, a decision MD Anderson said it would appeal. At issue was lost or stolen research data.

Although the situation obviously isn't a happy one for MD Anderson, the resulting detailed ruling provides a rare look at what led to the violations and reveals where the cancer center's efforts to fulfill its HIPAA obligations fell short, at least in the eyes of the administrative law judge (ALJ) in the case.

Struggling to comply with HIPAA is a near universal endeavor for covered entities (CEs), but it may be especially complicated for institutions that conduct research, such as academic medical centers and colleges and universities with medical schools.

"I've often said in the 20 years that I've been dealing with HIPAA that I believe [the intersection of] HIPAA and research is one of the most complex areas of HIPAA," Marti Arvin, vice president of audit strategies for the security consulting firm CynergisTek Inc., told *RRC.*

The passage of time "absolutely has not" improved the situation, added Arvin, whose previous positions include chief compliance officer for the University of California Los Angeles (UCLA) Health and chief privacy officer for the University of Louisville.

In his 17-page ruling, ALJ Judge Steven T. Kessel shot down a number of MD Anderson's explanations and defenses for why it should not have to pay the multimillion-dollar fine, including that, as research data, the lost information wasn't protected health information (PHI) and thus not subject to HIPAA (*RRC 8/18, p. 1*).

Three incidents that occurred from 2012-2013 triggered the initial OCR investigation; all involved unencrypted data:

◆ The director of research informatics at the Genitourinary Cancer Center reported the theft from his home of a laptop containing data for 30,000 individuals. MD Anderson had paid for the laptop so he could work from home.

◆ A summer intern in the Stem Cell Transplantation and Cellular Therapy Department lost a personally owned USB thumb drive onto which she had downloaded PHI for 2,264 individuals.

◆ A visiting researcher from Brazil was unable to locate her unencrypted thumb drive with data for 3,598 people.

Of MD Anderson's $4.358 million penalty, $1.348 million was assessed for failing to implement access controls, specifically encryption (and decryption). OCR considered MD Anderson not compliant from March 2011 to Jan. 25, 2013, in this regard. The $3 million balance of the fine was imposed for the impermissible disclosures stemming from the missing thumb drives and the laptop.

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

This document is only available to subscribers. Please log in or purchase access.

Purchase Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.