

Report on Medicare Compliance Volume 33, Number 10. March 18, 2024 Lack of Risk Analysis Cost NY Hospital \$4.75M; OCR Issues Warning

By Theresa Defino

Although the HHS Office for Civil Rights (OCR) described its recent \$4.75 million agreement with a Bronx, New York, hospital as settling a “malicious insider cybersecurity investigation,” the agency considered a total of 11 breaches Montefiore Medical Center experienced from 2010 to 2022 in establishing sanctions, *Report on Patient Privacy* (RMC’s sister publication) has learned.

As with many other OCR investigations that lead to settlements, the lack of a risk analysis was a central finding in this case and figured in a \$40,000 agreement the agency also issued last month. In a related development, OCR Director Melanie Fontes Rainer in late February announced the agency was launching a “risk analysis enforcement initiative,” although she provided few details.

Regarding the Montefiore settlement, the agency drew attention to an employee found in 2015 to have stolen the protected health information (PHI) of 12,517 patients and who later “sold the information to an identity theft ring.”^[1] It is not clear how or why this qualifies as a “cyber-attack,” as Fontes Rainer called it, rather than an ordinary employee-turned-criminal situation.

The employee acted over a six-month period in 2013, but the theft wasn’t discovered until 2015, following a tip from the New York Police Department.

“OCR’s investigation revealed multiple potential violations of the HIPAA Security Rule, including failures by Montefiore Medical Center to analyze and identify potential risks and vulnerabilities to protected health information, to monitor and safeguard its health information systems’ activity, and to implement policies and procedures that record and examine activity in information systems containing or using protected health information,” OCR said in its Feb. 6 announcement. “Without these safeguards in place, Montefiore Medical Center was unable to prevent the cyberattack or even detect the attack had happened until years later.”

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

[Purchase Login](#)