COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 24, Number 3. March 07, 2024 Montefiore's History of Breaches Preceded $4.75M OCR Settlement

By Theresa Defino

Montefiore Medical Center recently agreed to a $4.75 million settlement with the HHS Office for Civil Rights (OCR) following an investigation that found the Bronx, New York, hospital lacked a security risk assessment, didn't regularly review information system activity nor have mechanisms in place "that record and examine activity in all information systems that contain or use." [1]

OCR mentioned only one incident that triggered the settlement—namely a 2013 breach, discovered in 2015, involving an employee's theft of 12,517 patients' protected health information (PHI) that was sold to an identity theft ring.

But that theft is just one of Montefiore's 11 reports of breaches affecting 500 or more individuals that appear on OCR's reporting portal. Entities began submitting reports in 2009. Montefiore's first report was submitted March 9, 2010, and its most recent, as of *RPP*'s deadline, is from Sept. 23, 2022. In total, 142,119 patients were affected. Seven of the 11 were the result of employee misdeeds; just one involved a business associate (BA).

Breaches reports posted online include the date submitted to OCR, the number of individuals affected, whether a BA of the covered entity (CE) was involved, the type and a list of actions the organization took in response. For Montefiore, several use the same vague description of those actions. Entries also list involvement by OCR if any occurred.

Montefiore's reported breaches posted online, from the oldest submission to the most recent, are as follows:[2]

- **March 9, 2010**: 625 individuals affected; theft of an unencrypted laptop from the medical center's mobile dental van. The laptop contained "included names, dates of birth, medical record numbers and dental x-rays. Upon discovery of the breach, the CE filed a police report and provided breach notification to HHS, the media and affected individuals. As a result of OCR's investigation, the CE revised its procedures so that all [electronic] ePHI is stored in a data center rather than the mobile dental van laptop. In addition, the CE encrypted all mobile dental van laptops and improved physical security for the van. The CE developed a new policy on ePHI security and retrained all staff. OCR obtained assurances that the CE implemented the corrective action listed above."

- **July 23, 2010**: 16,820 individuals affected; theft of two unencrypted desktop computers. "The ePHI included medical record numbers, dates of birth, admission/discharge dates, billing codes, and social security numbers. Upon discovery of the breach, the CE filed a police report and provided breach notification to HHS, the media, and affected individuals. It also provided substitute notification by posting on its website. As a result of OCR's investigation, the CE replaced its building alarm and installed bars on the windows. In addition, the CE directed its staff to save patient data only on a centralized network drive, moved all ePHI stored on desktop hard drives to centralized secured network servers, and encrypted all of its computers. The CE also revised its policy and procedure on password management and provided training to all staff on its new policy."

- **July 23, 2010**: 23,753 individuals affected; theft of three unencrypted desktop computers. OCR investigated

the theft. "The ePHI included names, medical record numbers, dates of birth, parent or guardian contact numbers, asthma diagnoses, vaccination information, and number of visits to the school health clinic. Upon discovery of the breach, the CE filed a police report and provided breach notification to affected individuals, HHS, and the media. As a result of OCR's investigation, the CE updated its building alarm to include additional motion sensors and installed surveillance cameras. Further, the CE encrypted all of its computers, advised that no ePHI is stored on desktop hard drives, removed all ePHI from its computers, and stored ePHI on the centralized secured network servers. The CE also revised its policy and procedure on password management and provided training to all staff on its new policy."

- **July 22, 2015**: 12,517 individuals affected. This is the breach that led to the $4.75 million settlement. The website entry does not list the details of the breach. As described in the settlement agreement, an employee inappropriately accessed patient account information from Montefiore's electronic medical record (EMR) system and sold "certain" information to an identity theft ring.

- **Sept. 14, 2020**: 76,068 individuals affected. This is described as a hack/information technology incident involving Montefiore's network but was the result of a ransomware attack experienced by an unidentified BA. "The ePHI involved included names, addresses, dates of birth, and treatment information. The CE notified HHS, affected individuals, the media, and provided substitute notice."

- **Sept. 18, 2020**: 4,004 individuals affected; unauthorized access/disclosure by an employee. According to Montefiore's public breach announcement, the employee stole the PHI from January 2018 to July 2020 and was fired; at the time, it said, "There is no evidence that this patient information has been used for identity theft."[3] As reported on the OCR website, the PHI stolen "involved included names, dates of birth, addresses, health insurance information, and partial Social Security numbers. The CE notified HHS, affected individuals, the media, and posted substitute notice on its website. In its mitigation efforts, the CE strengthened its administrative, technical, and security safeguards to better protect its sensitive data."

- **Dec. 1, 2020**: 670 individuals affected; unauthorized access/disclosure of paper/films by an employee. "The PHI involved included names, dates of birth, addresses, health insurance information, and partial Social Security numbers. The CE notified HHS, affected individuals, the media, and posted substitute notice on its website. In its mitigation efforts, the CE strengthened its administrative, technical, and security safeguards to better protect its sensitive data."

- **Jan. 29, 2021**: 1,670 individuals affected; unauthorized access/disclosure from the EMR by an employee. "The PHI involved included names, dates of birth, addresses, health insurance information, and partial Social Security numbers. The CE notified HHS, affected individuals, the media, and posted substitute notice on its website. In its mitigation efforts, the CE strengthened its administrative, technical, and security safeguards to better protect its sensitive data."

- **April 13, 2021**: 943 individuals affected; unauthorized access/disclosure from an EMR by an employee. The PHI involved included names, dates of birth, addresses, health insurance information, and partial Social Security numbers. The CE notified HHS, affected individuals, the media, and posted substitute notice on its website. In its mitigation efforts, the CE strengthened its administrative, technical, and security safeguards to better protect its sensitive data."

- **April 22, 2022:** 3,717 individuals affected; unauthorized access/disclosure from an EMR by an employee. "The PHI involved included names, dates of birth, addresses, email addresses, phone numbers, health insurance information, and partial Social Security numbers. The CE notified HHS, affected individuals, the media, and posted substitute notice on its website. In its mitigation efforts, the CE strengthened its

administrative, technical, and security safeguards to better protect its sensitive data."

- **Sept. 23, 2022**: 1,332 individuals affected; theft of an employee's USB drive. "The PHI involved included names, dates of birth, email addresses, medical record numbers, diagnoses, and other clinical information. The CE notified HHS, affected individuals, the media, and posted substitute notice on its website. In its mitigation efforts, the CE provided complimentary credit monitoring services and strengthened its administrative, technical, and security safeguards to better protect its sensitive data."