Report on Patient Privacy Volume 21, Number 2. February 04, 2021 Excellus Agrees to Pay $5.1M, Implement CAP To Settle OCR Investigation From 2015 Breach

By Jane Anderson

Excellus Health Plan Inc., based in Rochester, New York, agreed to pay $5.1 million and implement a two-year corrective action plan (CAP) to settle alleged violations related to a breach that was discovered in 2015 but dated back to 2013. The massive breach exposed protected health information (PHI), including Social Security numbers and claims data, for more than 9.3 million members over the course of nearly 17 months.[1]

The investigation by the HHS Office for Civil Rights (OCR) found multiple potential violations of the HIPAA rules, including failure to conduct an enterprise-wide risk analysis, and failures to implement risk management, information system activity review, and access controls, the agency announced Jan. 15. The two-year CAP requires a full risk analysis, a risk management plan, and development and distribution of policies and procedures. In a statement to *RPP*, Excellus officials noted that no finding of actual violations was made.

"Hacking continues to be the greatest threat to the privacy and security of individuals' health information," said then-OCR Director Roger Severino in a statement.[2] "In this case, a health plan did not stop hackers from roaming inside its health record system undetected for over a year which endangered the privacy of millions of its beneficiaries....We know that the most dangerous hackers are sophisticated, patient, and persistent. Health care entities need to step up their game to protect the privacy of people's health information from this growing threat."