COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 19, Number 12. December 04, 2019 'Misinterpretation' of Breach Rule, Lack of Internal BAA Cost Hospital Group $2.1M

By Theresa Defino

Sentara Hospitals, a nonprofit group of 12 medical centers in Virginia and North Carolina, will implement a fairly minimal two-year corrective action plan (CAP)[1] and pay the HHS Office for Civil Rights (OCR) nearly $2.2 million, a surprisingly high amount for what the organization refers to as a single billing "error." OCR Director Roger Severino, however, used unusually strong language in announcing the settlement a day before Thanksgiving, accusing the hospitals of misinterpreting what constitutes a breach and refusing to comply with reporting requirements even when warned.

Sentara's settlement, which also concerns the alleged lack of an internal business associate agreement (BAA), is the third enforcement action OCR issued[2] in a single month and among the speediest complaints it has formally resolved.

According to OCR's Nov. 27 announcement, the $2.175 million settlement was triggered by a complaint it received April 17, 2017, that "Sentara Hospitals sent a bill to the complainant with another patient's protected health information (PHI) enclosed." The agency offered no explanation for how it arrived at the settlement amount nor why a CAP was necessary. OCR typically requires CAPs when it finds an organization has multiple HIPAA violations, such as failing to conduct a security risk analysis, which it did not find in this case.

OCR said Sentara "reported this incident as a breach" that affected eight people, while the agency's investigation "determined that Sentara mailed 577 patients' PHI to wrong addresses that included patient names, account numbers, and dates of services."

The agency contended that Sentara "concluded, incorrectly, that unless the disclosure included patient diagnosis, treatment information or other medical information, no reportable breach of PHI had occurred." OCR added in the announcement that Sentara "persisted in its refusal to properly report the breach even after being explicitly advised of their duty to do so by OCR."

Said Severino: "HIPAA compliance depends on accurate and timely self-reporting of breaches because patients and the public have a right to know when sensitive information has been exposed. When health care providers blatantly fail to report breaches as required by law, they should expect vigorous enforcement action by OCR."