KRIEG DEVAULT

Insights

Failure to Report HIPAA Breaches Results in Costly Fine and Corrective Action Plan

February 4, 2020

By: Stacy Walton Long and

Sentara Hospitals (Sentara) entered into a $2.175 million settlement and corrective action plan with the Office of Civil Rights (OCR) under the U.S. Department of Health and Human Services (HHS) for alleged violations of the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA).

HHS received a complaint in April 2017 which alleged that Sentara sent a bill to a patient with another patient's protected health information (PHI) enclosed. Sentara performed a risk assessment and reported that only eight patients were affected by this unauthorized disclosure. However, OCR's investigation revealed Sentara improperly mailed PHI to 577 Sentara patients.[1] Sentara improperly concluded that it was under no obligation to report this breach because the breach did not involve the disclosure of patient diagnoses or treatment information.[2] Moreover, Sentara failed to cooperate with OCR despite being informed of its duty to report the breach.

OCR's investigation also revealed Sentara had not entered into a business associate agreement (BAA) with its parent corporation, Sentara Healthcare. Further, Sentara permitted Sentara Healthcare to provide services that involved the disclosure of PHI without obtaining proper assurances under HIPAA.[3] Many providers may not understand or properly comply with the BAA requirements associated with separate but related legal entities such as subsidiaries or sister corporations.

In addition to the monetary settlement, the corrective action plan requires Sentara, among other obligations, to develop, maintain, and revise, as necessary, written policies and procedures to comply with HIPAA breach notification standards. Sentara's incident is a prime example of the importance of understanding the Privacy and Security Rules under HIPAA, and the reporting obligations in the event of a HIPAA breach.

OCR Director, Roger Severino, stated: "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."

If you have questions regarding HIPAA breaches, reporting obligations, HIPAA requirements for entities sharing ownership or control, or other HIPAA-related questions, please contact Stacy Walton Long, Alexandria M. Foster, or any other Krieg DeVault attorney in the Health Care Practice Group.

[1] https://www.hhs.gov/sites/default/files/signed-ra-sentara-508.pdf.

[2] https://www.hhs.gov/about/news/2019/11/27/ocr-secures-2.175-million-dollars-hipaa-settlement-breach-notification-and-privacy-rules.html/.

[3] *Id.*