Chris Bennington
Partner
Cincinnati
513.870.6572
cbennington@bricker.com

HIPAA settlement highlights importance of mobile device encryption

July 28, 2020

On July 27, 2020, the U.S. Department of Health and Human Services (HHS) announced that it reached a settlement with a Rhode Island nonprofit health system related to the theft of an unencrypted laptop containing its patients' protected health information (PHI). Lifespan Health System Affiliated Covered Entity agreed to pay $1,040,000 and to adopt a corrective action plan with two years of monitoring by the HHS Office for Civil Rights (OCR).

In 2017, Lifespan filed a breach report with OCR concerning the theft of a hospital employee's laptop containing PHI that included patient names, medical record numbers, demographic information and medical information. In all, the laptop contained the PHI of over 20,000 patients.

OCR opened an investigation in response to the breach report and determined that there was systemic noncompliance with HIPAA regulations, including a failure to encrypt laptops even after Lifespan had determined it was reasonable and appropriate to do so. The investigation also uncovered a lack of device and media controls and a failure to have a business associate agreement in place with related entities. "Laptops, cellphones, and other mobile devices are stolen every day, that's the hard reality. Covered entities can best protect their patients' data by encrypting

mobile devices to thwart identity thieves," said Roger Severino, OCR Director.

This settlement announcement should serve as a reminder to all HIPAA covered entities of the importance of mobile device encryption. While the Security Rule's Implementation Specification for encryption is "addressable," covered entities must utilize encryption if it is reasonable and appropriate to do so. Further, under the Breach Rule, covered entities are only required to make notifications for breaches of unsecured PHI. Devices that are encrypted as specified in the Security Rule are "secured," and a covered entity is therefore not required to issue notifications when an encrypted device is lost or stolen.