Insights

Failure to Encrypt Mobile Devices Results in a $3 Million Mistake

February 4, 2020

By: Stacy Walton Long and

The University of Rochester Medical Center (Rochester) settled with the Office of Civil Rights (OCR) for $3 million for repeated violations of the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA) relating to its failure to encrypt ePHI on mobile devices. This settlement was one of OCR's largest settlements in 2019.

In 2013, Rochester reported a breach to OCR when an unencrypted flash drive containing ePHI was lost. In 2017, Rochester reported another breach to OCR when an unencrypted personal laptop of a resident surgeon containing ePHI was stolen. OCR began its investigation after these two reported breaches, and found that Rochester impermissibly disclosed the ePHI of 43 in 2017.

The majority of the $3 million settlement was not due to the 2017 breach. Instead, it was due to Rochester's *continued failure* to comply with HIPAA regulations throughout the years. OCR's investigation revealed that Rochester's alleged HIPAA violations began in 2010 when it contacted OCR for technical assistance for a similar breach involving an unencrypted mobile device. Specifically, from 2010 to 2017, Rochester failed to:

- conduct accurate and thorough risk analyses of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all of the ePHI it held;
- utilize security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with HIPAA rules;
- implement policies and procedures that govern the receipt and removal of hardware and electronic media containing ePHI into and out of a facility, and the movement of these items within the facility; and
- enact mechanisms to encrypt and decrypt ePHI, or alternatively, document why encryption was not reasonable and appropriate and implement an equivalent alternative measure to encryption to safeguard ePHI.[1]

In addition to the monetary settlement, Rochester must comply with a two-year corrective action plan. The corrective action plan requires Rochester to conduct an accurate and thorough risk analysis, develop and enact a risk management plan, implement a process for evaluating environmental and operational changes, and amend and follow sufficient policies and procedures to ensure HIPAA compliance.[2]

It is imperative that a healthcare provider conduct risk analyses, implement policies and procedures, and utilize security measures to safeguard ePHI and comply with HIPAA. Failure to do so may cost you millions!

If you have questions regarding HIPAA compliance policies, 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] Resolution Agreement between Rochester and OCR: https://www.hhs.gov/sites/default/files/urmc-ra-cap-508.pdf

[2] *Id.*