The Price of Unencrypted Devices: *$1M Fine for Stolen Laptop*

Prepared by:
Joshua A. Mooney
White and Williams LLP

Published on www.lorman.com - December 2020

LORMAN®

Lorman Education Services is a leading provider of online professional learning, serving individuals and teams seeking training and CE credits. Whether you're looking for professional continuing education or an enterprise-wide learning and development solution, you will find what you need in Lorman's growing library of resources.

Lorman helps professionals meet their needs with more than 100 live training sessions each month and a growing collection of over 13,000 ondemand courses and resources developed by noted industry experts and professionals.

Learn more about Lorman's individual programs, economical All-Access Pass, and Enterprise Packages:

www.lorman.com

The Price of Unencrypted Devices: $1M Fine for Stolen Laptop

Written by: Joshua A. Mooney

One side effect of the COVID-19 pandemic on data security is that the sudden need to convert the workplace from onsite to remote operations potentially has required many organizations to use older equipment or personal devices that lack proper encryption. The use of such devices, combined with the lack of having proper controls in place to secure workplace data, can incur significant liability. Although involving an incident that pre-dates the pandemic, a settlement agreement entered into between the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and Lifespan Health System Affiliated Covered Entity (Lifespan ACE), subject to a July 27, 2020 OCR press release, serves as one example. Under the settlement, which arose from the theft of an unencrypted laptop containing protected health information, Lifespan ACE agreed to:

- pay a fine in excess of $1 million, and
- implement a "corrective action plan" that includes two years of OCR oversight and monitoring.

In February 2017, a hospital employee's car was broken into while parked in a public lot, resulting in the theft of a MacBook laptop used by the employee for work purposes. It is unclear

whether the laptop was provided by the hospital or whether it was a personal device. The encryption settings on the hard drive had not been set — meaning the hard drive and the data stored on it were unencrypted. Lifespan ACE determined that the employee's work emails may have been cached on the device's hard drive, and that through the cached emails, the thieves could have access to both patient names and medical records. In addition, the hard drive may have included information about patients across various affiliated providers.

Following an April 21, 2017 breach report filed by Lifespan ACE with OCR, the agency commenced an investigation of the healthcare provider. That investigation determined that there was "systemic noncompliance" with data privacy and security requirements under HIPAA, including "a failure to encrypt ePHI on laptops after Lifespan ACE determined it was reasonable and appropriate to do so." OCR also determined that Lifespan ACE lacked "device and media controls," and failed "to have a business associate agreement in place with the Lifespan Corporation," the healthcare provider's parent company. In particular, the consent settlement agreement noted:

A. Lifespan did not implement policies and procedures to encrypt all devices used for work purposes (see 45 C.F .R. § I 64.312(a)(2)(iv));

B. Lifespan did not implement policies and procedures to track or inventory all devices that access the network or which contain ePHI (See 45 C.F.R. § 164.3 10(d)(l));

C. Lifespan did not have the proper business associate agreements in place between Lifespan Corporation and the Lifespan healthcare provider affiliates that are members of the Lifespan ACE (See 45 C.F.R. § 164.502(e)); and

D. Lifespan impermissibly disclosed the PHI of 20,431 individuals (see 45 C.F.R. § 164.502(a)).

What's notable are both the size of the fine assessed against LifeSpan ACE and that the incident spawned from the theft of a single laptop. In a post pandemic world that requires a remote workforce and virtual operations, a simple precaution of ensuring that all devices used by employees could slip through the proverbial cracks. Thus, when issuing laptops or other devices to employees, or when otherwise contemplating employees' use of personal devices for work-related functions, organizations must ensure the encryption of workplace data. Here are some simple solutions to consider:

- Use of a central enterprise program to manage data encryption of all work-issued devices. Such programs should be setup to override a user's ability to inadvertently or intentionally disable the data's encryption.
- Management of access tools and applications, such as for email, that prevent a user's ability to transfer data from a workplace network to the hard drive of the personal device used to work remotely. If the

data cannot be stored on a personal hard drive, the need to encrypt workplace data is obviated.

- Implementation and enforcement of policies and procedures that prohibit the storage of workplace data on the hard drive of a personal device. These policies should be acknowledged by employees on an annual basis, at minimum, and be enforced.
- Controls that encrypt any data transferred from the organization's network to removable media, like a thumb drive or CD.
- Teach employees how to arm encryption protocols on personal devices.

If you have questions or would like further information, please contact Joshua A. Mooney (mooneyj@whiteandwilliams.com; 215.864.6345).