COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 29, Number 28. August 03, 2020
Lifespan Pays $1M to Settle HIPAA Case Over Stolen Unencrypted Laptop

By Nina Youngstrom

The 2017 theft of an unencrypted laptop is at the heart of a new HIPAA settlement[1] with Lifespan Health System Affiliated Covered Entity (Lifespan ACE) in Rhode Island, which agreed to pay $1.04 million to settle potential violations of the privacy and security rules, OCR said July 27.[2]

It reinforces the importance of encryption, although generally health care organizations have gotten the message, said Brian Selfridge, a partner in Meditology Services and CORL Technologies. They should be focusing on the security risks posed by business associates and other third parties, which is a growing threat because of the unrelenting outsourcing by health care organizations.

Lifespan ACE includes three academic teaching hospitals—Rhode Island Hospital and its Hasbro Children's Hospital; The Miriam Hospital; and Bradley Hospital—as well as Newport Hospital and Gateway Healthcare. According to Lifespan ACE's resolution agreement with OCR on Feb. 25, 2017, a MacBook was stolen from the car of a Rhode Island Hospital employee. Lifespan ACE realized the employee's work emails possibly were cached in a file on the laptop's hard drive, and the thief may have had access to patient names, medical record numbers, demographic information and the names of one or more medications that were prescribed to patients. Protected health information (PHI) on the laptop may have included patient information from Rhode Island Hospital, Lifespan Pharmacy LLC, retail pharmacies and affiliated Lifespan ACE hospitals, OCR said.

Lifespan Corp., the parent company and business associate of Lifespan ACE, reported the breach, which affected 20,431 people, to OCR on April 21, 2017. OCR investigated and concluded "there was systemic noncompliance" with HIPAA, including a failure to encrypt devices used for work. OCR also said it found "a lack of device and media controls" and no business associate agreement between Lifespan Corp. and the Lifespan ACE providers.

The laptop hasn't been recovered. In a statement, Lifespan said there's been no indication that patient information has been accessed or used by anyone because of the laptop theft. "Lifespan takes these situations very seriously and deeply regrets the incident occurred. Both prior to the incident and over the past three years we have taken several steps to further enhance our tactics to protect the security and confidentiality of patient information." The resolution agreement includes a corrective action plan. Lifespan did not admit liability.

That was in 2017, and by now, it should be obvious to organizations that encryption is a necessity, Selfridge said. "Based on what I've seen coming out of OCR over the past 10 years, encryption is king," he said. "If you have a list of 100 things you need to correct, encryption of devices is number 1 or 2." He said the technology has gotten cheaper and easier to deploy, especially with Microsoft BitLocker encryption technology and a wide range of affordable encryption options for MacBooks, so most organizations have a handle on it. "We still see some organizations trying to figure out USB encryption," Selfridge said.

Third-Party Risks Loom Large

He thinks they should have pivoted to the risks posed by third parties because of the volume of vendors. "It used to be you would outsource a handful of things, but now even small systems have hundreds of vendors they share PHI with," Selfridge explained. They include medical device vendors, financial services companies, cloud computing companies, business intelligence analytics companies, law firms, revenue cycle consultants and supply chain companies—many of them the business associates (BAs) of the hospital. "Health care organizations are relying—for the majority of critical IT infrastructure—on third parties and business services, and that arena has become the biggest exposure not only for compliance but just the potential for you to lose availability of critical systems if those organizations experience a security breach," Selfridge said. The vendor could be the victim of a ransomware attack, for example, which also could jeopardize the hospital's clinical and operational functions.

Although BAs are obliged to comply with HIPAA privacy and security rules and could face an OCR enforcement action, that may not move them to invest in cybersecurity adequately, Selfridge said. "The biggest motivators we have seen for BAs to get religion on security is if it's in the contract with the health systems," Selfridge said. They require business associates to get security certifications, such as HITRUST and SOC 2. "That's the number one lever that drives security for BAs. If you're aligned with HITRUST certification criteria, you're in excellent shape for HIPAA compliance."

Contact Selfridge at brian.selfridge@meditologyservices.com.

1 HHS, "Lifespan Resolution Agreement and Corrective Action Plan," June 26, 2020, https://bit.ly/39xzN59.
2 HHS, "Lifespan Pays $1,040,000 to OCR to Settle Unencrypted Stolen Laptop Breach," news release, July 27, 2020, https://bit.ly/33g8CuR.