Compliance Lessons From $1M HHS Fine For Data Breach

By **Stacy Harper, Shannon Bond and Hillary Martel** (August 14, 2020)

Stacy Harper

Shannon Bond

Hillary Martel

The Office of Civil Rights in the U.S. Department of Health and Human Services continues to penalize covered entities for breaches of patients' electronic protected health information, or ePHI, under the Health Insurance Portability and Accountability Act privacy rules.[1]

In a recently published press release, the OCR announced that Lifespan Health System's affiliated covered entity entered into a settlement agreement with the OCR, wherein Lifespan agreed to pay $1.04 million and enter into a corrective action plan as a result of a data breach affecting 20,431 patients.[2]

The ePHI included patient names, medical record numbers, demographic information, including partial address information, and the name of one or more medications that were prescribed or administered to patients.

Upon seeing the settlement amount and number of patients affected, some might, at first glance, believe the settlement amount to be out of proportion for a breach only affecting 20,431 patients.[3]

However, the OCR seems to be prioritizing protective measures taken by covered entities rather than the volume of ePHI that was breached. For Lifespan, even though only 20,431 patients' ePHI was breached, the OCR's investigation revealed that Lifespan failed to take basic measures to protect ePHI from a breach, and the OCR took stronger steps as a result.

The Breach

How did the breach occur? Lifespan's scenario could happen to anyone: An employee's car was broken into and a laptop that the employee used for work purposes was stolen from the car and never recovered. Lifespan self-reported the stolen laptop and the breach of ePHI.

While that scenario seems blameless — the breach did not occur because the employee left the car unlocked, used public Wi-Fi, erroneously sent ePHI via personal email, etc. — Lifespan itself was not blameless because it failed to enact organizational and structural precautions to prevent even blameless breaches of ePHI.

In its investigation, the OCR found that Lifespan:

- "[D]id not implement policies and procedures to encrypt all devices used for work purposes";

- "[D]id not implement policies and procedures to track or inventory all devices that access the network or which contain ePHI"; and

- "[D]id not have the proper business associate agreements in place between the Lifespan Corporation and all other provider affiliates that are a part of the [associated covered entity]."

Encrypting devices, being aware of devices that contain or can access ePHI, and putting business associate agreements in place are standard measures that covered entities take to remain HIPAA compliant.

So, although the manner in which the breach occurred was blameless, the framework established by Lifespan that allowed a blameless loss of equipment to become a breach made Lifespan blameworthy.

The Settlement

As a result of Lifespan's breach of ePHI, it agreed to pay $1.04 million to HHS. It also entered into a corrective action plan requiring Lifespan, among other requirements, to:

- Enter into business associate agreements with existing business associates.

- Revise its policies and procedures to designate a person to manage and monitor agreements with, and the appropriateness of entering into, business associate agreements.

- Implement encryption and access controls for all devices used for Lifespan's business.

- Report to the OCR (1) the total number of devices and equipment that may be used to access, store, download or transmit ePHI; (2) the total number of encrypted devices; (3) reasons for not encrypting any devices; and (4) how Lifespan is controlling access to its network.

- Revise its policies and procedures as they pertain to device control and access.

- Train or retrain all Lifespan personnel who have access to ePHI and obtain certification from each that he or she has completed the training.

- Submit annual reports regarding Lifespan's compliance with the corrective action plan.

The Takeaways

Covered entities are well aware that they maintain, and their personnel has access to, highly sensitive information about patients. They are also aware that they have a duty to protect that highly sensitive information from spreading to those who should not have access to it. The hard work lies in the implementation of protections and the process of vigilantly enforcing and evolving those protections, as needed.

The OCR is not implementing severe penalties in every situation and recognizes that some breaches will occur. However, the OCR expects that certain baseline measures must be implemented by a covered entity to protect ePHI.

The settlement agreement with Lifespan also makes it clear that if reasonable precautions are not implemented, even where the number of patients affected is relatively limited, the OCR will take strong action to let the covered entity at issue, and all other covered entities, know that the quality of protections, not the quantity of those affected, is most important. If a covered entity takes all reasonable precautions to protect ePHI, the OCR will be less likely to take as harsh an action against that covered entity.

Covered entities and business associates should heed the OCR's warning and implement baseline measures to protect PHI:

- Perform risk assessments as required under HIPAA regulations to ensure systems and safeguards for the protection of PHI are reviewed and reassessed, at least annually, to ensure they are working appropriately and not outdated. Where risks are identified, modify systems and safeguards to respond to the risk.

- Implement processes to manage business associate arrangements, including execution of the business associate agreements that clearly establish responsibility and specifically address any compliance concerns and or requirements.

- Train and continually reeducate employees on HIPAA-compliant protocols, so they properly adhere to HIPAA privacy and security requirements.

- Implement encryption for all systems and devices that use and store ePHI and maintain an inventory to track these systems and devices. It is not enough to simply put a few security measures in place.

In its press release, HHS stated that the:

> OCR's investigation determined that there was systemic noncompliance with the HIPAA Rules including a failure to encrypt ePHI on laptops after Lifespan determined it was reasonable and appropriate to do so.

Lifespan failed to take basic precautions to protect ePHI — encrypting devices, being aware of devices that contain or can access ePHI and putting business associate agreements in place.

As a result of Lifespan's breach of ePHI, the OCR made a clear statement with the settlement agreement that organizational and structural effort must be made to protect ePHI and that, if it is not, the OCR will have an undeniably strong response. Through implementation of baseline security measures, other organizations can avoid this outcome.

Stacy Harper is a partner, and Shannon Bond and Hillary Martel are associates, at Spencer Fane LLP.

Spencer Fane partner Shawn Tuma contributed to this article.

[1] "HIPAA Privacy Rules" includes all federal standards that govern the privacy of individually identifiable health information (45 C.F.R. Part 160 and Subparts A and E of Part 164), the Federal standards that govern the security of electronic individually identifiable health information (45 C.F .R. Part 160 and Subparts A and C of Part 164), and the Federal standards for notification in the case of breach of unsecured protected health information (45 C.F.R. Part 160 and Subparts A and D of 45 C.F.R. Part 164).

[2] Lifespan Pays $1,040,000 to the OCR to Settle Unencrypted Stolen Laptop Breach, HHS Press Office (July 27, 2020), https://www.hhs.gov/about/news/2020/07/27/lifespan-pays-1040000-the OCR-settle-unencrypted-stolen-laptop-breach.html. Lifespan Resolution Agreement and Corrective Action Plan, HHS.gov, https://www.hhs.gov/sites/default/files/lifespan-ra-cap-signed.pdf.

[3] By contrast, in May 2019, a settlement agreement with a diagnostic medical imaging services company agreed to pay $3,000,000 to settle a HIPAA breach affecting 300,000 patients. Tennessee diagnostic medical imaging services company pays $3,000,000 to settle breach exposing over 300,000 patients' protected health information, HHS Press Office (May 6, 2019), https://www.hhs.gov/about/news/2019/05/06/tennessee-diagnostic-medical-imaging-services-company-pays-3000000-settle-breach.html.