SpencerFane®

$1,040,000 HIPAA Settlement for Stolen Unencrypted Laptop Breach — Why?

The United States Department of Health and Human Services reached an agreement with Lifespan Health System Affiliated Covered Entity (Lifespan ACE) in which Lifespan agreed to pay $1,040,000 and adopt a corrective action plan in the wake of its data breach that exposed over 20,431 patients' protected health information. The breach occurred when an employee's unencrypted laptop was stolen which contained electronic protected health information (ePHI) including: patients' names, medical record numbers, demographic information, and medication information.

On the surface this settlement, like many other HHS settlements, may seem harsh when looking at only the amount of money vis-a-vis the number of patients affected. In the world of HIPAA breaches, and data breaches in general, 20,431 affected individuals is not a large breach. And for a stolen laptop? Laptops get stolen everyday, right?

It has become quite common for those who find themselves in the crosshairs of an HHS investigation to say that the agency acts too harshly and that the money HHS is fining companies would be better spent on those companies' security practices. Unfortunately, those who feel this way do not understand what HHS (and most other regulatory agencies) are trying to accomplish, which leads to the key takeaway from this settlement.

THE KEY TAKEAWAY

HHS is trying to get companies to comply with the law and, more broadly, their obligation to protect the sensitive information that people have entrusted to them.

We have handled numerous cases where HHS *could* have imposed penalties on companies but did not because it was clear that the companies were *being diligent* and *were trying* to get it right. They may not have gotten it right. There may have been breaches that exposed patients' information. But, they were *trying*.

Now, looking at HHS' actions through this lens, consider the following details HHS provided about the Lifespan ACE case:

- "OCR's investigation determined that there was systemic noncompliance with the HIPAA Rules including a failure to encrypt ePHI on laptops *after Lifespan ACE determined it was reasonable and appropriate* to do so."
- "OCR also uncovered a lack of device and media controls, and a failure to have a business associate agreement in place with the Lifespan Corporation."

"'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."

Mistakes happen every day. Everyone understands that when it comes to cybersecurity there is no such thing as being completely "secure." But, when an entity recognizes that it has significant vulnerabilities that are likely to lead to the compromise of the privacy of people's sensitive information, they have to take it seriously and act diligently in mitigating those vulnerabilities. They have to *try* to get it right. If they don't make a *good-faith effort*, they will likely pay a price for it when something bad happens.

This blog post was drafted by Shawn Tuma, a Partner in the Plano, TX office of Spencer Fane LLP. For more information, visit www.spencerfane.com.