Health Information Compliance Alert

Case Study: Secure Your Devices or Risk Hefty Penalties

Lost phone? It better be encrypted, OCR case suggests.

Just because a laptop is password-protected doesn't mean that you can avert a HIPAA breach. You must encrypt any and all mobile devices especially if you use them in the field. Unfortunately, one healthcare organization recently found out what happens when you don't keep your tools under lock and key.

Background: On February 1, 2017, Children's Medical Center of Dallas was fined $3.2 million for some HIPAA violations dating back to 2009 and 2013. The civil money penalty (CMP) ranked in the top ten of biggest fines that the Office of Civil Rights (OCR) and HHS ever bestowed on a healthcare organization.

Back in January of 2010, Children's Medical Center reported the loss of a BlackBerry at the Dallas/Fort Worth International Airport to the OCR. The unencrypted, non-password protected mobile device, which went missing on Nov. 19, 2009, "contained the ePHI of approximately 3,800 individuals," states the OCR press release from Feb. 1, 2017.

"With increasing frequency, HHS is announcing significant 6- and 7-figure settlements with covered entities and business associates," **Michael D. Bossenbroek, Esq** of Wachler & Associates, P.C. in Royal Oak, Michigan says. "These settlements, although they uncovered other problems, often originated with stolen or lost PHI."

Round two: Despite the implementation of some security measures, a second major breach occurred in April of 2013 after Children's discovered the theft of an unencrypted laptop that included the ePHI of 2,462 individuals.

"On July 5, 2013, Children's filed a separate HIPAA Breach Notification Report with OCR," the release says. And, while Children's did enforce a badged entry and had a security camera in place at one of the entrances, the healthcare organization didn't fully protect the area, allowing unauthorized staff access to the ePHI, the report suggests.

FYI: The largest HIPAA settlement was in August of 2016. Advocate Health Care, based out of Illinois, failed to protect the ePHI of its patients resulting in fines of $5.55 million to the HHS and OCR.

Get With the Program

Unfortunately, cases like this one are not unique and highlight the need for a comprehensive compliance plan. "OCR's vigorous enforcement of HIPAA has been on an exponential trajectory and the recent settlements are a harbinger of continued enforcement in 2017 and beyond," says **John E. Morrone, Esq**, a partner at Frier Levitt Attorneys at Law in Pine Brook, NJ. "The increase in the number of enforcement actions, and the severity of the fines associated with subsequent investigations, emphasize the need for HIPAA compliance."

Preparation matters. Thieves and hackers seem to always find new ways of accessing private information, especially when it comes to ePHI. One trend that continues to gain steam is the theft of ePHI via mobile platforms, and this type of breach can cost you millions.

"A comprehensive HIPAA Plan serves to reduce the risk of a breach, as well as mitigate potential fines in the event of a breach," Morrone explains. "Recent settlements indicate that OCR will continue to penalizeentities not only on the basis of a breach itself, but also for failing to have in place the requisite safeguards that HIPAA requires to limit and/or prevent such an occurrence."

Consider The Facts

As the OCR persists in its pursuit of HIPAA-compliance transgressors, it's mission critical that you keep abreast of the

issues that might cause a breach in your compliance wall. There were HIPAA warning signals at Children's Medical Center, but they were ignored and it cost the organization big time.

Red flags: The OCR's investigation revealed that "Children's noncompliance with HIPAA Rules" is what led to the violations, the announcement suggests. Specifically, OCR found that the medical center:

- Neglected to set up a risk management plan despite OCR recommendations to do so.
- Failed to utilize encryption and similar safeguards on "all of its laptops, workstations, mobile devices and removable storage media until April 9, 2013."
- Warned of possible risks as early as 2007 when it was discovered that unencrypted BlackBerry devices were issued to nurses.
- Subsequently caused the loss of 3,800 individuals' ePHI in 2009 and 2,462 individuals' ePhI in 2013.

Official response: "Ensuring adequate security precautions to protect health information, including identifying any security risks and immediately correcting them, is essential" said **Robinsue Frohboese**, OCR acting director in a prepared statement. "Although OCR prefers to settle cases and assist entities in implementing corrective action plans, a lack of risk management not only costs individuals the security of their data, but it can also cost covered entities a sizable fine."

Remember: The key is really assessing risk from the get go. "Many physicians don't understand that this is the first element in HIPAA security," says **Abby Pendleton, Esq.** of The Health Law Partners, P.C., in their Southfield, Michigan office. "This type of risk analysis is the starting point to find potential vulnerabilities and then put into place the appropriate safeguards. It is the stepping stone to implement HIPAA but not enough practitioners do it."

Tip: If you're not sure what is permissible under HIPAA, it might be a good idea to revisit the HIPAA Security Rule and audit your current compliance plan for irregularities. Read on to get started on your HIPAA compliance plan today.

Take a look at this HIPAA Security Rule guidance for your future reference: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.