Most Expensive Laptop Ever? $2.5M HIPAA Settlement Traced Back to Theft

With the undeniable shift from paper to pixels in the world at large – includ

the realm of healthcare – there's an ongoing discussion about cyber-security and protecting consumers' (and patients') sensit information. And ignorance about how to offer that protection is never a valid excuse in the event of a breach.

Stolen laptop reveals holes in provider's ePHI security

In a case recently settled with the U.S. Department of Health and Human Services Office for Civil Rights (OCR), a stolen lapt represented much more than the loss of business equipment…it was the catalyst for an investigation revealing a health servic provider's cloudy understanding of Health Insurance Portability and Accountability Act of 1996 (HIPAA) security requirements they apply to electronic protected health information (ePHI).

This week the OCR announced in a press release that Pennsylvania-based CardioNet, an organization that remotely monitors cardiac patients, agreed to settle alleged HIPAA noncompliance for $2.5 million and a promise to enter into a "corrective actio plan." The OCR reports that this outcome is the first HIPAA settlement to involve a provider specializing in wireless services.

Thousands of patients' protected health information made vulnerable

CardioNet alerted the OCR in January of 2012 that an employee's laptop – containing the ePHI of nearly 1,400 patients – was stolen from a car parked near the individual's residence. A month later, the provider filed a second report informing the OCR o breach of over 2,200 individuals' ePHI.

The OCR launched an investigation in the spring of 2012 into the organization's compliance with HIPAA's Privacy, Security, a Breach Notification Rules, and ultimately determined that "CardioNet had an insufficient risk analysis and risk management processes in place at the time of the theft."

Beyond the provider's inadequate risk protocol, the OCR found that CardioNet had not fully and correctly implemented the po and procedures required of the HIPAA Security Rule (they were in unimplemented draft form at the time of the incident). Additionally, CardioNet could not demonstrate that it had implemented any safety measures for securing ePHI, whether on portable devices or otherwise.

"Mobile devices in the health care sector remain particularly vulnerable to theft and loss," stated OCR Director Roger Severin an HHS press release. "Failure to implement mobile device security by Covered Entities and Business Associates puts indivi

sensitive health information at risk. This disregard for security can result in a serious breach, which affects each individual wh information is left unprotected."

Incomplete understanding about HIPAA requirements is biggest culprit

Although it's easy to point to the key risk as a laptop left in a parked car, the OCR's action paints a more detailed picture: the that CardioNet had an incomplete or hazy comprehension of what HIPAA truly required it to do in order to protect patients and consumers made all parties vulnerable. It's that lack of understanding the resolutions are aimed at correcting.

OCR stipulates two-year action plan to remedy CardioNet's "confusion"

Beyond the $2.5 million fee, the settlement between the OCR and CardioNet includes a Resolution Agreement to be carried o over two years. It will require CardioNet to undertake specific actions once an OCR-approved risk management plan is in plac including the following:

- Implement an employee training program (subject to the OCR's approval) regarding the use and security of mobile devi
- Inform the OCR in the event of a staff member's violation of any security policies or procedures;
- Furnish the OCR with yearly reports describing the corrective actions undertaken in the preceding months;
- Provide the OCR with certification that attests to the fact that all portable devices are properly encrypted;
- Regularly review company risk management rules and procedures with the goal of revising policies when necessary to a with Security Rule requirements (and provide the OCR with any revisions).

Clearly the tenor of these stipulations reflects the OCR's intent to be a hands-on presence as CardioNet makes the necessary fixes to become compliant with HIPAA security protocol.