Codify
BY AAPC

Health Information Compliance Alert

Case Study: Follow 3 Steps To Avoid Laptop HIPAA Breaches

OCR is pushing entities harder to perform risk assessments.

Two recently announced HIPAA settlements show that the **HHS Office for Civil Rights** (OCR) is cracking down on unprotected data contained on mobile devices. And if you're not already encrypting your mobile devices, you'll likely be next in the OCR's crosshairs.

Beware: HHS is Handing Down Tougher CAPs

Background: Stolen unencrypted laptops were to blame for two HIPAA cases, which totaled nearly $2 million in settlements, as well as extensive corrective action plans (CAPs). **Concentra Health Services**, a subsidiary of Humana, Inc., agreed to a $1.7 million settlement with HHS for alleged HIPAA violations related to a breach notification stemming from a stolen unencrypted laptop.

According to Concentra's HHS-ordered CAP, the company must:

- Implement a security management process, including a risk analysis and risk management plan;
- Provide written updates to HHS describing encryption requirements for all devices;
- Provide security awareness training for all workforce members;
- Submit an Implementation Report to HHS; and
- Submit Annual Reports to HHS.

QCA Health Plan, a health insurance provider in Arkansas, paid out a smaller settlement of $250,000, also due to a breach involving a stolen unencrypted laptop. The laptop contained the protected health information (PHI) of 148 individuals. Under QCA's CAP, the insurer must:

- Implement a security management process, including a risk analysis and corresponding risk management plan;
- Provide security awareness training for all workforce members who have access to electronic PHI (ePHI); and
- Submit Annual Reports to HHS.

These two breach cases share many similarities. Among them are three key steps these companies did not take that could have prevented the breaches in the first place or at least minimized the breach-associated costs and sanctions.

1. Make Encryption Your Best Friend

Crucial: The best precaution against a multi-million dollar settlement on your company's books is widely available encryption software, according to an April 24 blog posting by **Linn Foster Freedman** and **Kathryn Sylvia**, both Providence, RI-based partners with **Nixon Peabody LLP.**

Although encryption is not required by HIPAA, covered entities (CEs) and business associates (BAs) "should assure that portable devices, including mobile devices and laptops, are encrypted and contain the minimum amount of ePHI necessary for an employee to carry out his or her responsibilities if it is necessary at all," Freedman and Sylvia stated.

This high settlement amount indicates that CEs and BAs "who choose not to implement encryption standards must be able to explain themselves," wrote **Elana Zana** in an April 28 OMW Health Law blog posting for **Ogden Murphy Wallace Attorneys**, a law firm headquartered in Seattle. But there really is no other effective way for most providers to protect data other than encryption.

Loophole: "If a laptop or other mobile device is encrypted according to HHS standards, the loss or theft may fall within a

legal safe harbor," Freedman and Sylvia pointed out. "This fact alone should compel healthcare entities to consider using encryption technology."

2. Don't Make Excuses Perform a Risk Analysis

One of the big problems in this HIPAA breach case was, in addition to not encrypting the laptops, the entities didn't perform a risk analysis. You must "do a solid risk analysis," stresses **Jim Sheldon-Dean**, founder and director of compliance services for **Lewis Creek Systems, LLC** in Charlotte, VT.

Although unlike Concentra, QCA had no direct fault for failing to encrypt its laptops. Instead, the QCA settlement focused on its lack of sufficient HIPAA security policies and procedures, Zana explained. Specifically, HHS found that QCA failed to conduct a security risk assessment and failed to implement security measures, especially physical safeguards.

3. Implement a Risk Management Plan

Implementing a risk management plan is part of both settlement agreements, which should give you a good idea of how important this task really is. The CAP for QCA was different from Concentra's in that QCA's focused on workforce training and reporting of workforce noncompliance, rather than on encryption requirements, Zana noted.

Lesson learned: "The settlements reinforce the OCR's continued focus on enforcing failures to adequately protect ePHI on mobile devices," Freedman and Sylvia observed.

Like most breach cases, the simple solution is to encrypt the data to avoid an actual breach but these settlements reveal just how extensive your compliance obligations are and how severe the monetary penalties could be when you fail to protect PHI, Zana warned. "The message from HHS is not just the importance of data encryption, but rather its performance and follow-through with security risk analysis and implementation of security policies and procedures."

Concentra and QCA, like other healthcare organizations who have settled with HHS, will have years of compliance reporting obligations and security management requirements that will likely create significant cost burdens in addition to the monetary settlement," Zana concluded.

Link: To read the HHS press release and access the Resolution Agreements for both HIPAA settlements, go to www.hhs.gov/news/press/2014pres/04/20140422b.html.