Health Information Compliance Alert

Case Study: Learn 4 Lessons To Secure Your Backup Tapes

Delayed breach reporting can get you into even more hot water.

For HIPAA compliance, it may seem like you're encrypting everything these days from emails to laptops and other devices. But if you aren't also encrypting your data backup tapes, you're opening up your organization to a potentially serious breach risk. Here's how one hospital learned this lesson the hard way.

Background: On July 22, **Women & Infants Hospital of Rhode Island** (WIH) agreed to a consent judgment involving a $150,000 payment to resolve HIPAA breach allegations, according to a July 23 announcement by the **Massachusetts Attorney General's** (AG's) Office. The judgment resulted from a data breach that WIH reported to the AG's Office in November 2012.

The data breach exposed patients' names, dates of birth, Social Security numbers, exam dates, physicians' names, and ultrasound images. WIH has agreed to pay a $110,000 civil penalty, $25,000 for attorneys' fees and costs, and a $15,000 payment toward the AG Office's fund for education and future data security litigation. WIH also agreed to perform a review and audit of its security measures and to take any corrective measures recommended in the review, the AG Office said.

HIPAA expert and director of compliance services for **Lewis Creek Systems LLC** in Charlotte, VT Jim Sheldon-Dean offers the following four lessons that you can learn from this case:

1. Encrypt All Your Backup Tapes

In the summer of 2011, WIH shipped backup tapes from two of its Prenatal Diagnostic Centers to a central data center at WIH's parent company, **Care New England Health System**, according to the AG's press release. The backup tapes contained the protected health information (PHI) of 12,127 patients from the Centers, which are located in Providence, RI and in New Bedford, Mass.

Then, the parent company was supposed to ship the backup tapes off-site to transfer legacy radiology information to a new picture archiving and communications system. At some point during this shipping process, 19 unencrypted backup tapes went missing.

Crucial: One of the most important lessons to glean from this case is that you must encrypt your backup tapes, Sheldon-Dean stresses.

The missing backup tapes may not have posed such a serious HIPAA breach risk if they were encrypted. Unfortunately, WIH failed to encrypt the tapes.

"This case illustrates how important it is to ensure that any protected health information that is transported off site, including backup tapes, are properly protected through encryption or other secure means," advised attorneys **Kathryn Sylvia** and **Linn Foster Freedman** in a July 25 blog posting for the law firm **Nixon Peabody LLP.**

2. Put a Good System in Place to Manage Inventory

Problem: WIH had "an inadequate inventory and tracking system," which contributed to the hospital's alleged failure to discover that the tapes were missing until nearly one year later, the AG's Office charged.

Solution: "Have a good system for managing your backup tape inventory," Sheldon-Dean urges.

Under the settlement agreement, WIH agreed to maintain an up-to-date inventory of the locations, custodians and descriptions of unencrypted electronic media and paper patient charts containing PHI.

3. Beware of Transporting Over State Lines

In this case, the missing backup tapes contained PHI from Massachusetts residents, even though the transport originated from locations in both Rhode Island and Massachusetts. Therefore, WIH needed to report the breach to and comply with the breach-notification statute in Massachusetts.

Pitfall: "Recognize that you may have issues with other states when you have a breach and your patients are residents of other states," Sheldon-Dean points out.

4. Don't Drag Your Feet on Breach Reporting

What made matters even worse for WIH was the fact that the hospital failed to report the breach in a timely manner, Sheldon-Dean notes. Although the breach occurred in the summer of 2011, WIH didn't discover it until the following spring. Then, the hospital didn't report the breach until November 2012.

The AG's Office pointed to "deficient employee training and internal policies" as the cause of WIH's delay in properly reporting the breach.

Bottom line: And here's Sheldon-Dean's fourth lesson: "Don't delay reporting your breaches properly have a solid process!"