2 big HIPAA settlements show why hospitals must protect computers, PHI

Your hospital needs to make sure it's taking HIPAA compliance seriously, especially regarding its computers and networks. Any breaches or security problems involving patients' protected health information (PHI) can have significant consequences for facilities – including hefty fines from the Department of Health & Human Services' Office of Civil Rights (OCR). Two recent cases demonstrate just how much of an impact noncompliance can have on a hospital – and they also show which pitfalls your facility must avoid regarding PHI.

$5M mistakes

The first case involves the largest HIPAA-related settlement from a single covered entity. Advocate Health Care, an Illinois-based health system that includes multiple hospitals and a physician-led medical group, agreed to pay $5.5 million to OCR to resolve several data breaches.

According to a news release, a federal investigation into Advocate's HIPAA compliance began in 2013 after the health system reported three data breaches involving its physician-led medical group, which operates various outpatient, medical imaging, specialty and primary care offices.

Two of these breaches involved hardware theft, as discussed in an article from the *Chicago Tribune*. In one breach, four laptops containing unencrypted PHI were stolen from an administrative office. The second breach happened after another unencrypted laptop with the PHI of over 2,000 patients was stolen from an employee's unlocked vehicle.

The third breach involved a business associate of Advocate. An unidentified, unauthorized third party gained access to the business associate's network, which compromised the PHI of more than 2,000 Advocate patients.

After examining the circumstances behind these breaches, as well as Advocate's general privacy-related policies, OCR found that the health system failed to:

- conduct an accurate and thorough risk assessment for patients' PHI
- create policies and procedures to limit physical access to electronic information systems (including facility access controls)
- ensure it had written contracts from business associates outlining exactly how they were protecting PHI, and
- put reasonable safeguards into place to protect PHI in case of laptop theft.

Advocate said it was unlikely that any PHI was misused as a result of these breaches, and it's currently trying to fix the problems uncovered by the OCR investigation.

Weak password protection

The second big settlement was reached with one hospital and its affiliated facilities, as opposed to a health system. Because of multiple alleged violations (as detailed in a second news release), the University of Mississippi Medical Center agreed to pay $2.75 million to the feds.

Similar to Advocate, the University of Mississippi Medical Center's issues began with a laptop theft. However, after reporting the theft of the password-protected laptop to OCR as a possible data breach, further investigation revealed the hospital had bigger problems.

Any person could log into a password-protected hospital computer with a generic username and password, which provided immediate access to a network directory with thousands of files, including files with the electronic PHI for an estimated 10,000 patients, dating back eight years.

Because of this, the OCR investigation found that the hospital didn't:

- create policies and procedures to prevent and correct security violations
- implement safeguards for computer workstations to restrict ePHI access to authorized users only
- assign a unique username and password to each computer user to identify who has access to ePHI, and
- notify any individuals whose ePHI may have been compromised due to the hospital's neglect.

Even worse: The investigation uncovered evidence that the University of Mississippi Medical Center may have been aware of the vulnerabilities in its system for over a decade, yet did nothing to shore up the weaknesses until after the breach was reported.

As a result, the facility entered into the settlement with OCR, and it agreed to create a plan of action to correct these problems and boost its compliance with HIPAA laws.

Keys to protect your hospital

The biggest takeaway for hospitals here: Security is of utmost importance with computers used to access PHI.

All machines should be encrypted, and each staff member should have a unique username and password to access your system and patients' electronic medical records. In addition, staff should be trained on compliant computer usage and should exercise extreme caution when taking laptops or other hardware used to access PHI offsite.

Your hospital's efforts to keep electronic PHI safe should be specifically documented in your HIPAA risk assessment, and policies should be reviewed periodically with staff.

Putting in the work to ensure compliance now will help your facility avoid significant problems later.