Codify
BY AAPC

Health Information Compliance Alert

Case Study: Nip Your 'Unaddressed Risks' In The Bud Now -- Or Pay Dearly Later

Implement these 5 best practices right away to avoid this hospital's fate.

The scales are tipping drastically, and now an ounce of HIPAA prevention is easily worth at least a pound of "cure." This is especially true when that "cure" is in the multimillion-dollar range.

Case in point: On July 21, the HHS Office for Civil Rights (OCR) announced a $2.75 million settlement with the University of Mississippi Medical Center (UMMC) for multiple alleged HIPAA violations, including a breach. The UMMC includes University Hospital, which was the site of the breach.

Another Laptop at the Center of a Breach

Background: On March 21, 2013, UMMC's privacy officer discovered that a password-protected laptop was missing from the facility's Medical Intensive Care Unit (MICU), likely stolen by a visitor to the MICU who had inquired about borrowing one of the laptops, according to OCR. UMMC notified OCR of the breach, which triggered an investigation.

OCR's investigation revealed that users could access an active directory on UMMC's wireless network containing 67,000 files after entering a generic username and password. The director included 328 files containing the electronic protected health information (ePHI) of an estimated 10,000 patients, which made the ePHI stored on the UMMC network drive vulnerable to unauthorized access.

More problems: The investigation also revealed various other HIPAA violations, including that UMMC failed to implement its policies and procedures to prevent, detect, contain, and correct security violations. OCR also discovered that UMMC failed to implement physical safeguards for all workstations that access ePHI to restrict access to only authorized users, as well as assign unique user names and/or numbers for identifying and tracking user identity in IT systems containing ePHI.

"Finally, and significantly, the OCR found that UMMC failed to provide individual notification of the data breach," said attorney Linn Foster Freedman with Robinson & Cole LLP in a July 27 analysis. "As it failed to notify the individuals whose unsecured PHI was contained on the laptop and only provided notification on its website and through local media outlets."

What's more: OCR's investigation also uncovered UMMC's failure to undertake any significant risk management activities following the breach, despite being aware of risks and vulnerabilities to its systems dating back as far as April 2005. The lack of risk management activities was largely due to "organizational deficiencies and insufficient institutional oversight," according to OCR.

Identify Compliance Hot-Spots from This CAP

In addition to the $2.75 million payout, OCR also devised a corrective action plan (CAP) for UMMC, which will last for the next three years. Under the CAP, the UMMC must:

- **Internal Monitor:** Designate an internal monitor to ensure compliance with the CAP;

- Risk Management: Develop an enterprise-wide risk analysis and corresponding risk management plan that includes security measures to reduce the risks and vulnerabilities to ePHI to a reasonable and appropriate level;
- **Security Policy:** Update its Information Security Policy, and any necessary additional policies or procedures, to ensure compliance with the HIPAA Security Rule;
- Breach Notification: Revise its current Breach of Unsecured Protected Health Information Notification policy to state that the UMMC shall, following the discovery of a breach of unsecured PHI, notify each individual whose unsecured PHI has been, or is reasonably believed by UMMC to have been, accessed, acquired, used, or disclosed as a result of a breach as required by HIPAA;
- **Unique User ID:** Devise a plan to require a unique name and/or number to identify and track users of all information systems that contain ePHI, including departmental shared network drives;
- **Security Awareness & Training:** Provide its security awareness and training materials for all workforce members (including management) of its covered healthcare components who have access to ePHI, including specific training related to its new policies and procedures; and
- **Reportable Events:** Make a report to the internal monitor and HHS of any workforce member who may have failed to comply with its privacy and security policies and procedures or otherwise violated the HIPAA Privacy, Security, or Breach Notification Rules.

What You Can Learn from UMMC's Mistakes

The most important lesson you can learn from the UMMC settlement is that you "absolutely must conduct regular, comprehensive risk assessments of the risks to ePHI," urges New York City-based associate attorney **Ryan Logan of Hunton & Williams LLP**. "Several of the major HIPAA enforcement actions this year have emphasized the covered entity's lack of a risk analysis as a key factor that led to the incident."

"The risk analysis requirement has been in place for covered entities since 2005, and HHS published risk analysis guidance in 2010, so there is no excuse for covered entities (or business associates) to have not performed a risk analysis by 2016," Logan adds. Further, a risk analysis isn't complete without a corresponding risk management plan that implements safeguards to address the identified risks to ePHI.

Example: In the UMMC case, OCR specifically highlighted that UMMC failed to assign a unique user name/number to individuals with access to ePHI and even enabled access through a generic username and password, Logan points out. "Requiring a unique username for users with access to ePHI is an important technical safeguard that, as HHS notes, allows a healthcare entity to 'hold users accountable for functions performed on information systems with ePHI when logged into those systems.'"

Best practices: According to Freedman, you can also glean the following five additional lessons from this HIPAA breach settlement:

1. Update your policies and procedures to comply with the HIPAA Security Rule;
2. Confirm that physical safeguards are in place for workstations;
3. Confirm and update your security risk assessment and management policies and procedures;
4. Implement access control measures, including specific user names and passwords for access to PHI; and
5. Implement a breach notification policy that includes processes to notify individuals in the event of a data breach and follows the HIPAA breach notification requirements.

Lesson learned: In light of the hefty settlement amount and the various issues resulting in breaches and exposure of patient information cited in the resolution agreement, "compliance would have been WAY cheaper than the agreement, shall we say," stresses Jim Sheldon-Dean, founder and director of compliance services at Lewis Creek Systems LLC.

Link: To read UMMC's resolution agreement and CAP, go to www.hhs.gov/sites/default/files/UMMC_racap_508.pdf.

Codify
BY AAPC