Health Information Compliance Alert

Case Study: Malware Issue Highlights Large Organization Need for HIPAA Security Plan

Lack of firewall in secondary systems shows why risk analysis is crucial in healthcare settings.

Large organizations look at the big picture, forgetting oftentimes that it's a small chink-in-the-armor that renders a downfall. Such is the case involving the University of Massachusetts at Amherst (UMass), who despite the best intentions, fell victim to a HIPAA disaster after a malware issue left the organization vulnerable to ePHI loss.

Background. In a recent settlement, UMass agreed to pay $650,000 in a corrective action to the government for HIPAA violations that resulted from a malware virus on a workstation, which was uncovered during an investigation by the Office of Civil Rights (OCR) in June of 2013. The issue was detected on a workstation in its Center for Language, Speech, and Hearing also known as just "the Center" which resulted in the loss of ePHI at UMass and affected around 1,670 individuals.

The malware problem occurred because the university lacked a firewall to protect the information of the workstation users. "UMass failed to designate all of its health care components when hybridizing, incorrectly determining that while its University Health Services was a covered health care component, other components, including the Center where the breach of ePHI occurred, were not covered components," an HHS news release from Nov. 22, 2016 said.

HIPAA fail 101. What UMass failed to appreciate was the necessity for HIPAA compliance on auxiliary campus machinery. The Center lacked the written formalities that would have ensured the workstation coverage as a healthcare component under HIPAA, which is also known as hybridizing, the HHS news release suggests.

"HIPAA's security requirements are an important tool for protecting both patient data and business operations against threats such as malware," said **Jocelyn Samuels,** OCR director. "Entities that elect hybrid status must properly designate their health care components and ensure that those components are in compliance with HIPAA's privacy and security requirements."

Here's Why Risk Analysis Is Critical

Sadly, the Center did not perform a risk analysis until after the fact, and the failure to do so snowballed as UMass didn't have the technical safeguards in place to protect the people who used the workstation and their ePHI. Since the settlement, UMass has begun work on correcting its problems with "an enterprise-wide risk analysis" that will hopefully fix and manage future HIPAA dilemmas.

Tip: With risk analysis tools available through the HHS and reputable firms capable of quickly and efficiently assessing risk for healthcare facilities big and small, there's really no excuse for leaving data unprotected.

Here are five things you can do to combat HIPAA-related issues:

- Assess your HIPAA risk annually either with the HHS online tool or using a reputable firm or program.
- Hire a health IT provider who understands what's at stake under HIPAA and is certified.
- Test your software often for vulnerabilities and keep it updated.
- Ensure that your tech people are monitoring the firewall security.
- Look for antivirus products that protect against threats common to healthcare hacking.

To read the complete HHS news release, visit http://www.hhs.gov/about/news/2016/11/22/umass-settles-potential-hipaa-violations-following-malware-infection.html.

Codify
BY AAPC