Health Information Compliance Alert

Case Study: Design Your HIPAA Plan to Protect Against Threats Both External and Internal

Make sure your business associates understand the exit rules when employees leave.

What do small practices, big hospitals, multi-specialty clinics, physical therapy firms, DME businesses, and other healthcare entities have in common? They all have employees come and go. And if you don't have an exit strategy built into your HIPAA plan, then electronic protected health information (ePHI) can be compromised from the threat within.

Background: As a recent settlement indicates, one dangling thread can cause the whole operation to unravel.

Memorial Health Systems (MHS) is a non-profit, operating six hospitals, an urgent care center, a nursing home, and a variety of ancillary healthcare facilities in South Florida, in addition to having an Organized Health Care Arrangement (OHCA) with several physicians' offices. Due to a lack of clear-cut employee review procedures, MHS suffered the loss of ePHI on separate occasions that led to a $5.5 million settlement for HIPAA violations, a joint U.S. Department of Health and Human Services (HHS) and Office of Civil Rights (OCR) press release from Feb. 16, 2017 says.

The facts: Here's an outline of how MHS violated HIPAA from the HHS-OCR release:

- Ignored the risks of users and affiliated physicians' office users between 2007 and 2012 who had access to ePHI, failing to properly review terminated users' rights under HIPAA despite the advice from risk analysis to do so.
- Failed to notice the daily access of ePHI by a terminated employee whose credentials were not revoked, resulting in the loss of ePHI for over 80,000 individuals from 2011 to 2012.
- Reported the loss of "protected health information (PHI) of 115,143 individuals, which had been impermissibly accessed by its employees and impermissibly disclosed to affiliated physician office staff."

Was the Organization's Size a Factor?

Sometimes a small practice can be too trusting while a big healthcare group can be too busy to notice the day-to-day workings of its employees past and present. But it can be hard to justify these types of excuses with so many resources out there to help avoid HIPAA pitfalls. "While I think being busy or the 'that won't ever happen to me' logic may come into play," says attorney **Kathleen D. Kenney, Esq**., of Polsinelli LLP in Chicago. "Ultimately, I think this issue, like many HIPAA issues that arise, stems from a failure to implement processes and ensure checks and balances are in place when it comes to security."

Analyze Then Manage Your Risk

To avoid issues like those that tripped up MHS, your practice must first assess compliance shortcomings from reining in reception desk banter to multi-factor authentication on your mobile devices. But you need to scrutinize your findings in order to fully implement and manage a working HIPAA system. "We regularly see organizations with policies and procedures in place but they have stopped there," Kenney says.

Federal clarification: Your assessment should look at how a breach would "negatively impact" your practice's ePHI, suggests the HHS in its Q-and-A on the difference between risk analysis and risk management. When you analyze, you "consider all relevant losses that would be expected if the security measures were not in place," HHS notes. Management of that risk involves the way your practice implements HIPAA controls from the garnered information. Read the HHS Q-and-A here: https://www.hhs.gov/hipaa/for-professionals/faq/2013/what-is-the-difference-between-risk-analysis-and risk-management-in-the-security-rule/index.html.

"The implementation piece of HIPAA compliance is integral to breach avoidance," reminds Kenney. "OCR wants to see more than just documents on a shelf so taking the time to evaluate and carry out processes is key."

HIPAA go-to list: After you educate your current staff on insider threats, consider these compliance dos and don'ts for future employees and after employees move on:

- Do a comprehensive background check on future employees in regard to compliance issues.
- Do provide up-to-date materials on the changing compliance regulations for your staff.
- Don't forget to monitor your network and controls with tools that check log-on access and irregularities.
- Don't assume the "one-password-fits-all" mentality. Change your passwords often and implement multi-factor authentication.
- Do remember that the majority of breaches are caused from within an organization through employee oversight, accident, and theft of ePHI.

Reminder: MHS paid heavily despite its risk analysis due mostly to the lack of utilizing the data and ensuring only authorized users had access to the ePHI. "As this case shows, a lack of access controls and regular review of audit logs helps hackers or malevolent insiders to cover their electronic tracks, making it difficult for covered entities and business associates to not only recover from breaches, but to prevent them before they happen," said **Robinsue Frohboese**, OCR acting director in the release.