Codify
BY AAPC

Health Information Compliance Alert

Compliance: Consider this Violation Primer to Combat HIPAA Breaches

Tip: Encrypt your data - it's just that simple.

Fresenius Medical Care North America's (FMCNA) recent HIPAA issues highlight the need for risk assessment and management. Let's address the separate breaches and what you can do to fix problems like these before they bring down your practice.

1. Confirm physical safeguards are rock solid. Two FMCNA branches did not aggressively protect their locations from "unauthorized access, tampering, and theft" even though the HIPAA Security rule required them to do so, suggested an HHS Office for Civil Rights (OCR) release.

Ensure your practice has tight controls over not only electronics like workstations, laptops, mobile devices, and medical equipment to avoid illegal access, but also security for the facilities themselves that stop intruders from damaging and stealing equipment. Ask yourself these questions about the physical safety of your office and equipment:

- Is there a security system to protect the practice from unlawful entry?
- Are all devices inventoried?
- Is there a list of who has access to the building and the health IT?

Tip: "The high impact cases OCR moves forward with are intended to send a message to the industry," explains attorney **Kathleen D. Kenney** of Polsinelli LLP in Chicago, Illinois. "With that in mind, I advise our clients to use these cases as learning opportunities.

"Ask 'could this happen to my organization?'," Kenney stresses. "And, if the answer is 'yes,' use it as an opportunity to voluntarily take corrective measures."

2. Outline the access, movement, and removal of practice HIT. One of FMCNA's sites lacked the proper HIPAA protocols to fully protect its "hardware and electronic media that contain ePHI" from moving in, out, and around the facility, the OCR release mentioned. Consider these questions related to the "Administrative Safeguards" section of the HIPAA Security rule that specifically reference the movement and control of health IT:

- Have you designated an employee or staff as "security personnel" to oversee your risk management and the HIPAA compliance?
- Are your security protocols in line with your risk analysis and practice needs?
- Do your employees know who the compliance officer and health IT staff are?

Tip: "As devices get smaller and more portable, the potential for lost or stolen or misplaced data increases - and so does the risk for a breach," warns **Peter Arbuthnot**, regulatory analyst with American HealthTech in Jacksonville, Mississippi. That's why it's essential to clearly state who's in charge of the maintenance, care, and updates of practice technology.

3. Encrypt ePHI and maintain device control. More and more large-scale breaches fall prey to device management issues that lead to the loss of ePHI, and FMCNA failed to implement encryption strategies. When you encrypt and decrypt ePHI, set strong password protection on your mobile devices, and implement at-rest and remote access rules, you are protecting your patients and your livelihood. Check these three questions and see if you risk the exposure of ePHI:

- Is there a plan in place to protect your data if your devices go missing?
- Are you utilizing multifactor authentication and at-rest protocols for your devices?
- Is your data encrypted and decrypted appropriately, meeting Security rule standards?

Tip: "If you do have a breach in your networks, or if a device containing PHI is stolen, proper encryption can be a lifesaver," points out **Brand Barney, HCISPP, CISSP, QSA**, security analyst with Security Metrics in Orem, Utah. "If your data is properly encrypted using industry-accepted encryption strengths, you don't have a breach. And it's also a requirement for HIPAA."

Resource: For a closer look at the HIPAA Security rule, visit www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.