Health Information Compliance Alert

Case Study: Sometimes It's Risky Business to Take Your Work Home

The lack of applied safeguards on devices often leads to chaos.

Whether you load your briefcase with old-school files to review over the weekend or slip your tablet into your purse for a look-see at the beach, you gamble with your patients' privacy and security every time you remove patient data from the office.

Background: HIPAA violations aren't just for doctors anymore. The HHS Office for Civil Rights (OCR) and CardioNet, a cardiac-monitoring vendor who services patients at risk for cardiac arrhythmias, came to a settlement agreement for a breach from a stolen laptop in 2012. The theft led to the exposure of the electronic protected health information (ePHI) of 1,391 individuals, but the real culprit of the hefty $2.5 million fine compliance policies and procedures that weren't properly implemented, an HHS-OCR release from April 24, 2017 suggested.

See the HHS-OCR release at:
https://www.hhs.gov/about/news/2017/04/24/2-5-million-settlement-shows-not-understanding-hipaa-requirements-creates-risk.html

The heart-monitoring company failed to follow through on the HIPAA plans that it drafted, so when the laptop was stolen, it had no recourse. Laptops, phones, and tablets continue to put both providers and vendors at risk, accounting for many of the ePHI violations thus far in 2017.

Feds weigh-in: "Mobile devices in the healthcare sector remain particularly vulnerable to theft and loss," said **Roger Severino**, OCR Director in the statement. "Failure to implement mobile device security by Covered Entities and Business Associates puts individuals' sensitive health information at risk. This disregard for security can result in a serious breach, which affects each individual whose information is left unprotected."

Resolve Your HIPAA Issues Before Disaster Strikes

Accidents and thefts caused by human error do happen, and that's why it's critical to utilize your risk assessment and analyze it thoughtfully. What you uncover should be easy to translate into the management of HIPAA with policies and procedures to protect PHI and ePHI that everyone in your office can understand and implement. And that reach beyond just the privacy standards. Because with possible civil monetary penalties up to $1.5 million per breach, it's smart business to practice compliance whether you're in the office, at home, or on the run.

"We are constantly working with our clients, and they are always surprised at how much time it takes to be compliant," said **Rodney Murray, CISA, CRISC**, principal at IT Advisory at BHG in Charlotte, NC at HIMSS 17 in the "Managing Risk As a Business Associate" session. "The cost can add up really fast with a breach. Planning ahead is helpful, but those costs can turn big pretty quickly."

Breach defined: Quite simply, "a [HIPAA] breach is an improper or unauthorized use, disclosure, or access of protected health information (PHI)," explains **Cyndee Weston, CPC, CMC, CMRS,** executive director of the American Medical Billing Association (AMBA) in Davis, Okla.

HIPAA Breaches Aren't All Business- or Provider-Related

Though most breaches occur within the realm of a medical practice's business operations, some PHI and ePHI violations bleed into providers' and vendors' personal worlds. Incidents arise from things as varied as idle chit-chat, social media posts, or disregard for device controls and storage.

Important: According to Weston, when a physician shares a patient's medical history with a friend or family member that the patient has not authorized to access his medical records or information, it might be a breach. This will depend entirely on the situation, but everyone in the practice should mind what they disclose about patients' PHI outside of the office just to be safe.

Handle Remote Access Carefully

You don't necessarily need to stop bringing your work home, but you should definitely establish a policy on taking charts, computers, and other items that have patient data on them to any remote workplace. Unless handled very carefully, you could violate HIPAA and face penalties even if you just misplace one superbill in your home or forget your cell phone in a bathroom stall.

If you or your staff must take charts or other data, electronic devices, or any ambiguous materials that might contain PHI from the office, it's a good idea to implement a log-out system. That way, you'll know where each patient's information is, and there's some accountability should a breach occur.

Construct guidelines: Implement policies that require all practice personnel to safeguard any patient information when they remove it from the office, since the HIPAA laws protect the patient's privacy no matter where the chart happens to be. Consider these five things every time you take work from the office that includes PHI or ePHI:

- Were the files and devices logged out properly and approved by the administration under the aforementioned office HIPAA plan?
- Where can these materials and devices be securely stored at my remote location?
- Do my mobile devices, laptops, and at-home desktop computers include strong passwords with multi-factor authentication?
- Is encryption software utilized and updated for at-home or remote review of patient charts?
- Are the necessary resources readily available to alert compliance personnel should a breach occur while these materials are in my possession?

Tip: Enlist a reputable healthcare attorney or compliance consultant to ensure that all staff members are up-to-date on health IT privacy and security both at home and at the office.

Resource: If you're wondering what constitutes PHI, look at this list of 18 HIPAA identifiers at http://cphs.berkeley.edu/hipaa/hipaa18.html.