OASIS Alert

Patient Privacy: Beef up Your Laptop and Facebook Security Procedures

Take a closer look at these HIPAA security risks.

With HIPAA enforcement looking to ramp up in the near future, now's the time to make compliance with the patient privacy regulation a priority.

HHS Secretary **Kathleen Sebelius'** recent appointment of a former **Department of Justice** official to the top HHS Office for Civil Rights spot may indicate that providers can expect HIPAA enforcement to be on the rise, experts indicate. Former state and federal prosecutor **Leon Rodriguez** was chief of staff and deputy assistant attorney general for the DOJ Civil Rights Division before becoming OCR director. (OCR is in charge of enforcing HIPAA requirements.) And the health care reform law increased penalties for HIPAA violations, notes attorney **John Gilliland** with **The Gilliland Law Firm** in Indianapolis. The law also gave state attorneys general the right to enforce the patient privacy regulation.

"There's no question that HIPAA enforcement is increasing," Gilliland observes.

Home care providers may have a right to be nervous about increased enforcement, because they face HIPAA risks greater than those of facility-based providers. Home care providers are more vulnerable to breaches "because protected health information (PHI) is being taken outside the agency's office with its controlled access," Gilliland says. "The opportunities for breaches are more likely than when the PHI remains at one physical location with controlled security."

"The most serious breaches these days are caused by the loss or theft of laptops and portable devices such as CDs and memory sticks," points out **Jim Sheldon-Dean**, director of compliance services for information security consulting firm **Lewis Creek Systems** in Charlotte, Vt. "Home care providers tend to use a lot of portable data and devices, so their risks are greater."

Watch out: "It seems stolen laptops are becoming one of the most common breaches even though it is not difficult to avoid," Gilliland laments.

Home care providers face a double risk. "A home care provider has PHI in its office ... plus PHI being taken outside the office in conjunction with patient care," Gilliland tells **Eli**.

Solution: "Home care providers providers may want to consider encrypting mobile devices," says attorney **Kendra L. Conover, MHA** with Hall, Render, Killian, Heath & Lyman in Indianapolis, Ind. "While this is not a required standard under HIPAA, we have seen a recent trend in discussions with OCR and investigations that encryption is the gold standard that OCR expects providers to meet."

"Beyond standard HIPAA policies and procedures, home health providers may want to consider developing policies governing the use of mobile devices that contain or store PHI," Conover says.

Don't forget: HIPAA violations also can occur from unforeseen places, as one California hospital recently found out. **Stanford Hospital** in Palo Alto discovered that the names and diagnosis codes of 20,000 emergency room patients were posted on a commercial website, according to the New York Times.

The detailed spreadsheet that contained PHI was posted by a billing contractor to a website that allowed students to solicit help with schoolwork, along with a question asking how to convert the data into a bar graph. The attachment, which included six months worth of patient data from 2009, remained on the site for nearly a year until a patient discovered it and reported it to the hospital, which then removed the post and reported the breach.

Follow these Facebook Rules

Breaches via social media like **Facebook** are also a risk for home care providers, legal experts warn, since staff may develop close personal relationships with patients and forget to protect their PHI.

Home health agencies and hospices are susceptible to "inadvertent disclosure of PHI on social media, such as **Facebook**," cautions attorney Gilliland. "Field staff become close to the patients and then share information about them on social media, forgetting that social media is very public."

Remember that "social media is very public and that protected health information should never be posted -- that would be a HIPAA violation," Gilliland says.

"Individuals should not use their Facebook accounts to relate any personally identifiable information about their patients," emphasizes Sheldon-Dean.

Keep in mind that even if you don't mention the patient's name on a social media website, your posting could still pose a HIPAA violation risk if there is enough other information included to identify the patient, Conover says.

Consider the old World War II slogan, "Loose lips sink ships," in reference to social media, Gilliland suggests. Just as you wouldn't gossip about your patients in the grocery store, you shouldn't talk about them on Facebook.

Who Is Representing Your Agency?

In addition to hitting HIPAA concerns in training about Facebook, agencies should think carefully about how the organization will be portrayed through public posts. "Agencies ... should establish rules for how they are represented on Facebook, including who may represent the agency and what kinds of information may or may not be shared there," Sheldon-Dean recommends.

Do this: "Individuals should not represent the agency unless the agency has designated those individuals to do so, and they should be trained on the proper ways of being involved so as not to breach privacy," Sheldon-Dean counsels.

However, if an employee is "saying anything about the agency that could be considered an endorsement of the agency and/or its services, they should ID themselves as an agency employee," Gilliland advises.

Note: For more tips and strategies on running a successful home health agency, see Eli's Home Care Week. Information on subscribing is online at www.elihealthcare.com.