Health Information Compliance Alert

COMPLIANCE STRATEGIES: SHORE UP PRIVACY RULE COMPLIANCE WITH A PHI KIOSK

Don't forget--your patients have access rights too!

You may be so busy with other matters that you've put your patients' HIPAA-mandated right to access their PHI on the back burner.

Luckily, you can remedy that oversight with a networked, public computer station dedicated to patient use. But be careful: Without proper care your risks could outweigh all the benefits!

Allowing your patients to access their PHI via a networked computer could save your facility time and money, experts say. "Your patients want their information and you have to respond to that," reminds **Kevin Troutman**, an attorney at **Fisher & Phillips** in New Orleans.

And by working out the kinks in your patient PHI system early on, you may beat the rush while at the same time adding value to your patients' dollar.

However, as with any new use and access of PHI, you must weigh your facility's possible benefits against all the potential risks, experts remind.

Who's Entitled To What?

Allowing your patients to access their information via a PHI kiosk doesn't mean you have to allow them to see everything included in their records, asserts **Kirk Nahra**, a partner at Washington, DC's **Wiley Rein & Fielding**.

You have to ask yourself: "What do my patients want to see?" says Nahra. Typically, "patients don't want everything they're entitled to; they probably just want their last few visits," he explains.

Once you've narrowed down the types of information your patients are interested in, you can better protect the privacy and security of your PHI, Nahra says.

Accessing Access Risks

While experts agree that giving your patients the ability to access their PHI is risky, they admit that knowing your compliance risks can help you affirmatively manage potential privacy and security breaches.

Red flags: The obvious risks are threefold: password protection, physical privacy and security, and automated procedures to ensure patients log off before walking away, Troutman says.

Password Protection

"Their passwords need to be something besides their own personal identifying information," so that the system can authenticate the patients' identities, Troutman advises. Strong, complex passwords will go a long way in protecting that PHI, he adds.

Problem: If your patients don't practice "good password hygiene," all your controls will be useless, cautions attorney

Robyn Meinhardt of **Foley & Lardner** in Denver, CO. "Once patients are involved, you have far less administrative control, as they aren't necessarily complying with HIPAA," she reminds.

Solution: Educate your patients about how to safely access and manage their information. Example: Train your patients not to carry their passwords around with them or write them down," Meinhardt suggests.

By giving them the tools to keep their information private, you are saving both your patients and your facility from potential problems down the line, she says.

Physical Protection

"You must have a system to keep other people from seeing your patient's information on the screen, just like at an ATM," Troutman says. Tip: This physical protection could include a privacy screen or marking a line for the next patient to stand behind. You could also put the computer in a place that makes it hard for passers-by to see, he suggests.

Another component of this physical safeguard is deciding how patients are allowed to view their PHI, Nahra posits. Ask yourself: "Can they print their information or only view it on the screen?" he suggests.

"Presumably if patients sit down at the computer and print out their own information," they are then responsible for it, Nahra explains. However, "your facility must have some procedure in place to deal with misplaced information," he reminds.

Caution: If you decide to allow patients to print their PHI, "your printer needs to be located where only the person using the screen can have access to it," Troutman says. "And you probably need to provide a way for patients to destroy information once it's printed." Tip: Rather than just providing a trash can, put a shredder in the printing area, he says.

Logging Off

Meinhardt says the biggest problem she's seen is with logging out. Patients who aren't adequately trained are likely to leave the PHI kiosk without logging out of their accounts, she says. This can lead directly to strangers inappropriately accessing their PHI, she warns.

Combat this problem by having your system automatically log patients out of their accounts after a certain period of time with no activity, experts suggest. You can also remind patients at the sign-in screen that they are "being allowed access under certain circumstances and they are responsible for protecting their PHI by logging out," Troutman suggests.

The Bottom Line

Though your patients agree to assume responsibility, the PHI they are viewing is "still under your control and in your possession," Troutman reminds. That means you must apply stringent controls to ensure that the information is not inappropriately released to someone else, he says.

Remember: Your auditing needs will increase as patients begin using this system. "While there's an argument that any healthcare provider might need to see any patient's record, no patient should ever need to see another patient's record," Meinhardt stresses. An audit log will allow you to catch and mitigate any inappropriate disclosures.

The main benefit of this information station is that it saves time and permits quicker access to information, Meinhardt states. However, before you launch into this project, ask yourself the following questions:

• What information will our patients be able to see?

• How can we best protect their private health information?

• What can our patients to do with their information?

• Is this a viable long-term solution for us?

As always, document your processes in deciding whether PHI kiosks will work for your organization and then train your staff accordingly.