Health Information Compliance Alert

Privacy: Weigh Risks Against Benefits with PHI Portal Processes

A good log out procedure is just as important as a secure log in.

Your patients have the right to access their records. But you must ensure that the process you use to give patients access doesn't create problems down the line. Consider using a dedicated computer as a patient portal, but make sure to build in appropriate safeguards.

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. You have to ask yourself: "What do my patients want to see?" According to the **Department of Health and Human Services** (www.hhs.gov/ocr/privacy/hipaa/understanding/), "An individual's right of access generally applies to the information that exists within a covered entity's designated record set(s), including the following:

- a health care provider's medical and billing records
- a health plan's enrollment, payment, claims adjudication, and case or medical management record systems
- any information used, in whole or in part, by or for the covered entity to make decisions about individuals."

One way to give patients access to their files is to designate one computer in your practice as a patient portal. The obvious risks are threefold: password protection, physical privacy and security, and automated procedures to ensure patients log off before walking away, all of which you should consider in-depth.

Password Protection

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

Problem: If your patients don't practice "good password hygiene," all your controls will be useless. Once patients are involved, you have far less administrative control, as they aren't necessarily complying with HIPAA.

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. 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.

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.

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.

Another component of this physical safeguard is deciding how patients are allowed to view their PHI.

Ask yourself: "Can they print their information or only view it on the screen?"

Caution: Allowing patients to print the information leads to a new set of privacy concerns, since the papers could get lost or misplaced while still in your office. 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. And you probably need to provide a way for patients to destroy information once it's printed.

Logging Off

One of the biggest challenges is ensuring that a patient logs out of the system after reviewing his or her private information. Patients who aren't adequately trained are likely to leave the PHI kiosk without logging out of their accounts. This can lead directly to strangers inappropriately accessing their PHI.

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.

The Bottom Line

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

Remember: Your auditing needs will increase as patients begin using this system. No patient should ever need to see another patient's record. 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. 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. In addition, be sure you are aware of the current HIPAA laws regarding what your patients can and cannot access. Typically you can get this information from your practice's attorney or on the government's HIPAA website at www.hhs.gov/ocr/privacy.