Business Resources
by Category
Billing & Collections
Career Development
Coding
Finance
Human Resources
Legal
Operations
Strategy
Technology

< Home < Articles < Article Details

Search Site
GO

Need More Help?
Ask an Expert.

Technology: Privacy ... In Reality

Software can help with compliance, but watch out for those humans

By Theresa Defino

The doctor sent the test results to the office printer and instructed a staff member to take the printout, stick it in an envelope, and mail it to the patient.

Unfortunately, the staffer grabbed a bit more off the printer that day. No one realized that she'd sent the patient a portion of another patient's medical file until an official with the federal Office for Civil Rights (OCR) called to say it was investigating a complaint against the practice.

It is every practice's fear. In the rush and hustle of a busy office, a patient's health information is accidentally disclosed to someone who shouldn't have access to it. And that someone complains. To the federal government.

Could the practice have prevented this event? Not with all the newest gadgets, gizmos, and technology in the world. The lesson: No matter how good your IT is, violations of privacy and security rules most often result from simple human error.

That doesn't mean you should turn your back on technology. But if you purchase technology for compliance reasons, you should make sure you really need it and that it's worth the price you pay. It's also wise not to focus on making efforts just for the sake of satisfying a rule. Instead, put in place safeguards that will help keep you from reading about your office's privacy or security breach in the local paper.

The privacy rule requires that covered entities, including physician practices, safeguard what is known as "protected health information" (PHI) and take steps to limit disclosure only for purposes of treatment, payment, and healthcare operations. Even then, only the minimum amount of information needed by a recipient may be shared. The principal exception to this "minimum necessary" standard is when PHI is shared among clinicians for the purposes of treatment.

For its part, the security rule requires safeguards only for PHI that is stored or transmitted electronically. Practices must conduct a risk analysis, evaluating any threats to the confidentiality, accessibility, and integrity of their patient data.

Scant enforcement

You may well remember all the hype leading up to the enforcement date of the privacy rule. Many practices purchased a flood of products and services out of fear. Much less of a frenzy accompanied the security rule's implementation — partly due to lack of enforcement of the privacy rule.

But the government seems to have been even more lax when it comes to enforcing the newer security rule.

More than 18,000 complaints of possible violations of the privacy rule have been filed with OCR in the nearly three years since it took effect. But in the 14 months since the government began enforcing the security rule, a mere 50 complaints have been lodged.

In Summary

While you might be tempted to assume that all your privacy and security compliance issues can be solved by technology, you're only half right. To get the most out of your IT:

- Review what your system can already do, such as password protect documents and encrypt data before you buy additional products.
- Consider investing in a secure web-based portal to exchange e-mails with patients.
- Don't neglect simple precautions like creating unique individual passwords, safeguarding against errant faxes, and guarding against accidental disclosures in the office.

So far there have been only two criminal convictions for privacy-rule violations (both individuals pled guilty), none for security-rule violations, and no entities are known to have been fined for violations of either rule.

"You aren't seeing any real enforcement," says John C. Parmigiani, a healthcare security expert in Ellicott City, Md. Parmigiani is a former director of Enterprise Standards, which oversaw the development of the security rule for the Centers for Medicare & Medicaid Services. "There are providers who are saying, 'Until we see something, we'll take our chances.'"

But it would be a mistake to view action to protect patients' privacy and security as simply "compliance issues," advises Robert Tennant, senior policy advisor for health informatics for the Medical Group Management Association (MGMA).

"There are many reasons why you need to follow the [privacy and] security regulation[s], and the very last reason is government enforcement," says Tennant. "You will probably never be fined. But does that mean your practice does not need to secure health information? Absolutely not."

Any breach that is made public, or even word of a call from OCR, can have long-term repercussions. "If patients lose confidence in the practice, it could harm your reputation," Tennant warns.

He says that while it's difficult to gauge how much attention physicians are giving the security rule, his sense is that most understand that they must comply with it, but many don't understand it. They may think, erroneously, that they've already met the requirements because some are similar to those in the privacy rule.

"A certain amount of caution is called for, bearing in mind that you don't have to have a high-tech solution for everything," Parmigiani says. "A lot of it is physical and administrative safeguards. From a physician's perspective, a lot of what you are trying to do is keep information away from eyes that don't need to see it, and make sure that office staff are trained and understand the reasons for and the procedures required to protect sensitive patient and healthcare information."

To get a real-world perspective on compliance, it's useful to review common healthcare tasks, such as e-mailing and faxing, and ask what role technology can play in ensuring both patient privacy and security.

To encrypt or not?

Many practices are either toying with the idea of communicating with patients via e-mail, or have gone headlong into the venture. The key thing to remember is that unless you take special precautions, no e-mail is secure.

So you must prohibit disclosing PHI in messaging, consider encryption, or turn to a Web-based e-mail retrieval system.

"The analogy is if you are sending unencrypted e-mail, it is like sending a postcard — everyone can read it," says Parmigiani. "And if you send it to a wrong address, to someone who doesn't have a need to know, you can't cancel it or recall it. Encryption is like putting a letter in a sealed envelope."

Some systems have been around for so long that they are in the public domain and are free, or nearly so. One such program is called Pretty Good Privacy, or PGP. The free version is called the GNU Privacy Guard, and it is available at www.gnupg.org.

Hushmail is another free product that will send encrypted e-mails between hushmail users. Another version is available for purchase for less than $100. More information can be found at www.hushmail.com.

Yet another option is PostX, which sells a variety of products that can encrypt all outgoing messages (and documents) or only those that

contain certain key terms. Recipients do not need special software to view their messages. For details, visit www.postx.com.

Kerber recommends transferring to a web-based e-mail system that will notify your patient or recipient that a message is waiting for him on a secure Web site where it can be retrieved. Another option is Medem, a vendor that provides secure online consultation services between providers and patients.

Some vendors are using a network to provide encryption and a Web-based portal to retrieve secure messages. Others are providing the same service through an ASP (application service provider) model. For small physician groups, an ASP may be the most economically feasible option.

"Look at the cost of maintaining your own system. Generally, most physician offices don't have an IT department, so if there is a problem you call the ASP," Kerber says.

But while an ASP solution might cost less, it does present a different set of problems. Physicians should be conscious of the physical and technical access controls implemented by their ASP. Kerber warns physicians not to take ASP security for granted.

"If I am using Joe's ASP, I want to know that they have a disaster recovery plan and how often they are doing back-ups," he says.

Fax risks

Most offices still conduct much of their business via fax, sending and receiving referrals, authorizations, precertifications, and the like. In addition to misdialed fax numbers, the machine itself, if left with unattended private records, can be a virtual magnet for privacy and security violations.

Low-tech steps can minimize such risks. Place a cover sheet on all outgoing faxes, putting any sensitive information on the second sheet only. Make sure each page contains the same disclaimer as your e-mails, indicating that the communication is privileged and that you want to be contacted in the event of a misdirection.

"If you are sending a fax, the important thing is to make sure the intended recipient receives it," says Parmigiani. "It is always a good idea to check the number before it goes out," He adds that "if the fax has PHI, call ahead and say, 'I am sending this.'"

Tennant recommends periodically erasing your fax machine's memory, especially when you discard the device.

New watchdogs on the block

Privacy and security should be on your mind if you're shopping for an EMR. If you go to a trade show or technology conference, it's easy to be swept away by vendors' sales pitches and their systems' bells and whistles without really knowing whether they will keep your patient data safe and secure.

But that will soon change, thanks to the collaborative efforts of healthcare organizations studying EMRs. In 2004, the American Health Information Management Association, the Healthcare Information and Management Systems Society, and the National Alliance for Health Information Technology, formed the Commission for Certification of Health Information Technology (CCHIT).

Hoping to jump-start the adoption of EMRs, CCHIT is developing a certification process to ensure compliance with a minimum set of functionality, security, and interoperability requirements. The group's web site is www.cchit.org.

CCHIT has secured funding and support from HHS, as well as from the American Academy of Family Physicians and the American College of Physicians. It is expected to issue its first seals of approval on EMR products this spring. The certification process will be voluntary and function much like the National Committee for Quality Assurance does for health plans and physician practices.

In addition, the Research Triangle Institute is working with a new group, the Health Information Security and Privacy Collaboration, to examine state privacy laws. Supported by the National Governors' Association, this multiyear initiative will address variations among state privacy laws and evaluate how products can be standardized to be interoperable and comply with overlapping or conflicting requirements.

Don't overlook simple precautions

One of the easiest ways to keep your computers safe from privacy leaks is to maintain basic virus and spam protection software. This helps ensure your data is consistently available and not corrupted. Most experts believe a custom product is not necessary. Your local office supply store should offer a variety of software packages available for under $100.

The main thing to remember is that all programs must be regularly updated to combat new threats, and full system scans should be run periodically to ensure nothing is getting through — and to eliminate what has.

The final security rule requires a unique user name but not a unique password. But security experts believe individual passwords are essential and should be changed often.

Some systems can be configured to prompt a change in password automatically. It's also important to teach your staff the basics on how to create passwords.

"A good password is not really a word. It's not your son's name, or your birth date," says Kerber. "It's a combination of letters, numbers and characters. One of the ways to create a password is to pick a phrase, like I like watching monkeys at the zoo. You take the first letter of each word, and ILWMATZ becomes your password." Combine that phrase with numbers and symbols to make the password stronger.

"How often you change passwords depends on the tolerance of your employees," says Kerber. "I would say at least every 60 days. And any time anyone leaves, be sure to deactivate the employee's access rights and have everyone change their password because sharing passwords is commonplace."

As Kerber points out, staff cooperation is essential to good privacy and security policies; simply relying on IT won't cut it.

"The technology exists," Parmigiani agrees. "The harder part is enhancing the person's perception of why it is important to care about this."

Theresa Defino is an editor at Physicians Practice. *She can be reached via editor@physicianspractice.com.*

This article originally appeared in the June 2006 issue of Physicians Practice.