Alan Nessman, JD, of the American Psychological Association (APA) Practice Directorate knows how a lot of professional psychologists react when the subject of ensuring the privacy of electronic health records comes up: They either fall asleep, or they panic.

“There’s all this jargon,” admits Nessman, senior special counsel for legal and regulatory affairs. “It can feel like 10 techno-geeks got together to write the rules.”

But while security issues for electronic health records can seem daunting, psychologists shouldn’t be intimidated, says Nessman. Nor should they ignore the issue, thinking, “Well, I haven’t seen the HIPAA police take anyone off in handcuffs, so I’m not going to worry about it,” he says.

Instead, practitioners should familiarize themselves with the terminology involved, take some easy steps to protect their patients’ privacy and reach out for help as needed.

“My message is that there are simple ways to do it,” says Nessman.

Understanding the lingo

The first step is simply to understand the terms used in the realm of electronic health records, says Stacey Larson, JD, PsyD, the APA Practice Directorate’s director of legal and regulatory affairs. The directorate fields many calls from psychologists asking even the most basic question: What is an electronic health record?

Basically an electronic version of all of a patient’s paper records brought together in one place, electronic health records focus on a patient’s total health. They are designed to be “interoperable,” meaning they can be shared with other health care providers. If used meaningfully, she says, they can improve the accuracy of diagnoses and quality of care, improve coordination among all the health care providers patients see and even lower practitioners’ costs, thanks to savings from reduced paper use and office space.

Don’t confuse electronic health records with office management software, adds Larson. While both are electronic, office management software is designed to help practitioners with such tasks as appointment scheduling, messaging and billing. The key difference is office management software’s lack of interoperability, or the ability to exchange information with other health care providers.

It’s the interoperability of electronic health records that gives many professional psychologists pause, says Larson. Many fear that the very feature that makes it possible to share information with other providers also heightens the possibility that information will fall into the wrong hands.

Plus, professional psychologists are often confused by the language used in debates about electronic health records. Privacy, Larson explains, is a patient’s right to decide what information providers can share or should withhold. Confidentiality is the provider’s responsibility to protect that privacy. Security is the means by which providers achieve that goal of preventing unauthorized access.
Electronic health records are covered under the Health Insurance Portability and Accountability Act (HIPAA). Psychologists using electronic health records may not know it, says Nessman, but they’re required to comply with the HIPAA Security Rule. That means you must conduct a structured analysis of the various risks patient data could experience – such as unauthorized access or loss in a fire or flood – and take measures to protect against those security risks.

In January 2013 the federal government released the HIPAA Final Rule, which further enhanced patient privacy protections. (See “HIPAA Final Rule highlights for practitioners” in the March 14, 2013 issue of the PracticeUpdate e-newsletter at www.apapracticecentral.org/update/2013/03-14/final-rule.aspx.)

Take breach notification, for example. “It used to be that if information was encrypted, you didn’t have to worry,” says Nessman, citing a stolen laptop or hacked computer system as examples of potential breaches. After the compliance deadline of Sept. 23, 2013 arrives, however, a little more will be required.

Recognizing that the breach may be the work of a staff person who has the encryption key, the government now requires practitioners to perform a relatively simple risk assessment to determine if there is a low probability that protected health information was compromised. If the probability is higher, practitioners must alert the patients affected as well as the federal government. Except in cases where a staff member with the encryption key is suspected in the breach, encryption will generally save the practitioner from having to give breach notification because of the low risk.

The APA Practice Organization will provide further information to members on how to conduct this risk assessment, and how to adapt to other key changes in the HIPAA Final Rule before the September 2013 compliance deadline.

**Putting security in place**

You can’t just ignore all this and hope for the best, warns Nessman, acknowledging that the rules are extremely complicated.

For one thing, the government has stepped up enforcement efforts. In previous years, he says, the government seemed to only investigate major breaches involving hundreds of thousands of records. These days, they’re actually on the lookout for problems and have even made examples of a few small providers. “An ounce of prevention is worth a ton of cure,” he says.

The government is especially interested in practitioners who haven’t even invested that ounce of prevention, says Nessman. “The highest penalties are for people who haven’t tried to do anything,” he says. “People who haven’t taken any steps to comply: Wake up.”

And take the detailed, comprehensive approach required by the Security Rule, he says. The following tips can get you started, and will be important components, but they will not result in a practitioner being fully compliant:

- **Cover the basics.** Make sure home and office wireless connections are password-protected, says Nathan Tatro, project manager for practice research and policy in the Practice Directorate. When wireless connections aren’t secure, he warns, “A smart hacker could use your wireless connection to track keystrokes from your computer.” Similarly, if you’re using a mobile device to communicate with patients, make sure all data are encrypted, lock the device with a password and set it to go into locked mode if a few seconds go by without use. There are even applications that allow you to remotely erase your device’s files if it has been lost or stolen. And you should probably go ahead and delete text messages from patients after you’ve read them, says Tatro, urging practitioners to limit what information they keep on mobile devices in the first place.
Keeping Electronic Health Records Private and Secure  continued from page 11

- **Encrypt your data.** Encrypting protected health information to government standards will protect your patient’s privacy if you experience a breach. In fact, says Nessman, “Encryption is becoming the standard of care.”

- **Take advantage of built-in safeguards.** Electronic health records have built-in features to help safeguard information, says Tatro. With access controls, for example, you can decide what staff members should have access to which information. While an administrative assistant needs to be able to schedule appointments and code for billing, that person shouldn’t have access to a patient’s full record. Audit functions allow you to see who has accessed what information and when.

- **Maintain minimal clinical records.** “The whole point of electronic health records is that they’re easier to share,” says Nessman. “But that greater ease of sharing means that electronic health records are more likely to be read by a lot of people.” Be circumspect about what you put in an electronic health record while still providing information other health care providers need to better coordinate care and understand the value psychology brings. Keep the minimal clinical record appropriate for release in most circumstances, he says, adding that third party payers and states may have requirements about what type of information practitioners must keep. If it is important to your practice to keep detailed notes, Nessman recommends keeping separate psychotherapy notes inside or outside of the EHR. If kept within the EHR, they should be in a separate, clearly identified, more secure part of the electronic health record or in an electronic format outside the electronic health record system. “If you’re really old school, you can have them on paper,” says Nessman.

- **Focus on the risks you can control.** The average practitioner isn’t going to be able to confirm, for example, that a cloud storage vendor has the right encryption standards, says Nessman. Instead of worrying about highly technical issues, he says, focus on things you can control – such as how protected health information gets from your office to the cloud. Other processes that practitioners can control are the use of passwords and staff training.

- **Get help.** The APA Practice Organization has resources that can help you comply with regulations for safeguarding electronic health records. The HIPAA Security Rule primer and other materials available at Practice Central – apapracticecentral.org – can help you better understand the security rule. Members also can contact the APA Practice Directorate’s Office of Legal and Regulatory Affairs at praclegal@apa.org or 800-374-2723, ext. 5886. And while the APA Practice Organization does not endorse particular electronic health record products, says Tatro, staff can walk members through what they need and review several options.

Larson, for one, hopes that professional psychologists will use these tips to overcome any remaining fears about the privacy of electronic health records.

Says Larson, “Electronic health records can’t reach their full potential unless both patients and providers are confident that patients’ data are private and secure.”

NOTE: This article is based on a workshop presented during the March 2013 State Leadership Conference in Washington, D.C. sponsored by the American Psychological Association (APA) and the APA Practice Organization.