The increased use of laptops, tablets and smartphones as well as electronic health records in the health care arena has many benefits for health care professionals and patients. New technology allows for greater collaboration between providers to better serve their patients’ needs. It’s essential that psychologists using technology in their practice or weighing their options for doing so have a basic understanding of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

The Security Rule was designed with the recognition that technology and security threats change rapidly and that health care entities face very different risks to a patient’s health information, such as inappropriate access of protected health information (PHI) by staff, or accidentally sending PHI to the wrong person.

Psychologists and other providers need to comply with the Security Rule if they electronically transmit or store protected health information related to insurance claims or other third-party reimbursement. Doing this is called “triggering HIPAA.”

HIPAA’s Security Rule applies only to electronically transmitted or stored protected health information—known as ePHI—typically kept on computers or other electronic devices.

The Security Rule recognizes that security risks to ePHI cannot realistically be eliminated. Rather, the Rule is about taking reasonable measures to manage and reduce those risks in your practice.

Is your practice in compliance with the Security Rule under HIPAA?

The Security Rule outlines the steps providers must take to manage the risks of unintended disclosures of ePHI through security breaches such as hacking or improper access or accidental loss of ePHI through a computer crash, fire or flooding.

“Some practitioners think that they can comply with the Security Rule by taking a few simple steps like encrypting emails or adding password protection to their computer files,” says Alan Nessman, senior special counsel in the APA Practice Organization’s Office of Legal & Regulatory Affairs. “Unfortunately, that is not correct.”

Many health care providers, including psychologists, have expressed confusion on how to become and remain compliant with the Security Rule. “I don’t think most folks really do understand Security Rule compliance all that well,” says Joe Scroppo, PhD, JD, in Woodmere, New York, a risk management consultant for The Trust.

To comply with the Security Rule, psychologists must conduct a formal, structured risk analysis for their practice, determine the appropriate security measures needed, and implement those measures.

The basic approach of the Security Rule

The Security Rule does not require any single method or “best practice” for responding to all types of security risks.
Instead, the rule essentially requires psychologists to come up with reasonable security measures to respond to the risks identified in a risk analysis of the technology used in their practice and document the thinking behind the selection of those measures.

The rule also recognizes that the size of the health care entity affects its risks and responses. For example, a hospital is going to have different and more complex risks than a small group practice of psychologists. An independent practitioner does not have to be concerned about a large workforce and their access to a large system of computers and protected health information. Instead the solo psychologist may have to consider the training of an administrative assistant who takes care of appointments, and the risks posed to a few computers and other devices. A smaller practice may have to consider fewer variables, but it is no less important for that small practice to maintain security rule compliance.

**Conducting a risk analysis**

Psychologists must conduct a thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of any protected health information held or transmitted electronically by their practice. The rule details many types of risk to consider.

Your analysis should consider risks and vulnerabilities involving:

- Computers and any other electronic devices: desktops, laptops, smartphones, tablets, etc.
- Electronic file storage: hard drives, flash drives, electronic health records, cloud storage; and
- Electronic transmissions: whether submitting ePHI through a secure portal or sending emails to patients.

You should also consider how your office is set up. For instance, can patients walking through your office or sitting in the waiting room look directly at your computer screens and potentially see another client’s health information? If you employ staff, does the entire staff have access to all client records or just those portions relevant for their respective job duties? A risk analysis should also take into consideration how you plan to manage and train your staff to ensure the security of health information or ePHI that they may access.

Some questions that you should ask yourself as you are conducting your risk analysis are:

- Have you identified the ePHI within your practice or organization? This includes protected health information that you create, receive, maintain or transmit electronically.
- What are the external sources of ePHI? For example, do vendors or consultants create, receive, maintain or transmit ePHI?
- What are the human, natural and environmental threats to information systems that contain ePHI? This includes unauthorized/inappropriate access by staff, inadvertently sending ePHI to an incorrect recipient, the accidental downloading of a virus/malware by opening an unknown hyperlink or attachment, hacking by an unknown third party or natural threats such as floods and fire.

**Securing your practice**

After identifying the risks to ePHI in the risk analysis process, select appropriate security measures to manage those risks in your practice. Security measures include:

- Creating a system for backing up data and identifying data to backup
- Setting up systems and methods to limit staff access to certain data
- Determining whether to use encryption.

It is important to note that HIPAA does not require encryption. Encryption, however, does provide additional protection of health information that you store or transmit electronically. There are also encryption services available specifically for emails. As part of your risk analysis, it would be a good idea to document that you considered encryption—even if you ultimately decide encryption is not a good fit for your practice.

Additionally, if a breach occurs encryption will spare you the stress of having to alert or send breach notifications to affected patients, the Department of Health and Human Services and, if required by your state law, your state attorney general or other law enforcement.
Practitioners who have been found in violation of the HIPAA Security Rule after a breach has occurred have sometimes had to pay several thousand dollars in fines and notify several hundred patients.

**Implementation/documentation**

Once you have completed your risk analysis and considered the different options to take to best protect your practice, you must document thoroughly. When drafting your Security Rule compliance plan, you should show:

- the areas of risk you identified;
- the security measures you considered; and
- the final decision you made that will allow you to best protect your practice.

The process of analyzing the risks to your practice will be an ongoing one. The Security Rule does not spell out how often practitioners need to update the security measures, but it does say it should be done “as needed.” The frequency of updating your security rule compliance plan will vary with the size of your practice and your risks. Practices with greater risks and resources may do this annually.

Some events would trigger the update of your risk analysis:

- one or more security breaches;
- adding new or more technology to your practice;
- disposing of any device, technology or a significant volume of files; or
- insufficient security measures.

**What are the risks of non-compliance?**

Not complying with the Security Rule increases the risk of a security breach. Protected health information could be hacked, stolen or lost. We believe that security breaches – which trigger your obligation to notify patients and HHS – are how most practitioners’ HIPAA problems to come to light. Breaches often result in HHS conducting a comprehensive review of other aspects of a practice’s HIPAA compliance. Finally, breaches affecting more than 500 patients put the practitioner’s name on HHS’s published list—known as the “Wall of Shame” to members of the health care industry—where HHS lists practitioners who have suffered large security breaches.

In addition to breaches, a psychologist’s lack of Security Rule compliance can be revealed through complaints by patients to HHS and HHS audits.

**Audits.** The HHS Office for Civil Rights began ramping up audits last year and enforcement actions have continued this year. Some of these audits are random—practitioners are “picked out of a hat.” Some of the audits may be more selective, where a practitioner is chosen from a group of practitioners who have reported a past breach.

**Fines.** The minimum HIPAA fine increases depending on whether the practitioner knew they were out of compliance and whether he/she promptly took steps to fix it.

Practitioners who make no attempt to comply with the Security Rule open themselves up for the highest penalties: a minimum penalty of $50,000 per violation.

HHS has levied large multi-million-dollar HIPAA fines under presidential administrations that are viewed as pro-consumer, and administrations that are viewed as pro-business and anti-regulation. HHS has also levied fines against both large and small practices. Fortunately, HHS also has discretion to waive the HIPAA fine, and instead educate the practitioner who violated the law on proper Security Rule compliance.

**Still not sure if your practice is Security Rule compliant?**

The Office of the National Coordinator for Health Information Technology offers a free risk assessment tool at healthit.gov/providers-professionals/security-risk-assessment-tool for healthcare providers who want to assess their federal compliance.

Sherry Delaney contributed to this article.