Privacy Rule Compliance Is Not Enough: Three Things You Should Know about the HIPAA Security Rule

Chances are you have taken steps to comply with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. But compliance with the Privacy Rule does not make you compliant with the latest rule to go into effect — the Security Rule.

Security Rule compliance involves an entirely separate process to secure all patient information that is electronically stored, generated, transmitted or received. This includes related information such as patient notes, insurance records, email, or even a paper fax you send that is received via someone else’s computer.

As of April 20, 2005, psychologists deemed in violation of the HIPAA Security Rule could be subject to substantial penalties, including fines and even imprisonment.

Here are three important things every psychologist should know about Security Rule compliance:

1. The HIPAA Security Rule requires its own set of compliance activities.

Although there is some overlap, each HIPAA Rule is separate and distinct and requires its own compliance process. Under the Security Rule, if protected health information is transmitted electronically or stored on a computer, you must take specific steps to ensure that unauthorized parties cannot access that information. In other words, while the Privacy Rule outlines the process for obtaining authorized disclosures of protected health information, the Security Rule focuses on preventing unauthorized disclosure. A separate set of steps must be taken to ensure compliance with both.

2. Security Rule compliance requires more than adding new locks and a password.

To be compliant with the Security Rule, you must conduct a formal risk assessment of your practice, document your compliance decisions, and then implement safeguards to minimize any risks you have identified. Documenting the process of identifying and minimizing risks is as important as the actual steps you take. A psychologist responding to a Security Rule complaint will be required to demonstrate that he or she not only undertook a risk assessment, but also provide a rationale for why he or she did or did not choose to comply.

continued on page 10

Consumers remain concerned about the privacy of their personal health information. According to a 2005 national survey conducted by the California Healthcare Foundation, 67% of consumers are “somewhat” or “very concerned” about the privacy of their personal medical records.
Privacy Rule Compliance Is Not Enough:  
Three Things You Should Know about the HIPAA Security Rule  

Even if you do not submit electronic claims, complying with the Security Rule is sound risk management.

Like the Privacy Rule, the Security Rule is “triggered” when you transmit information in electronic form in connection with a “standard transaction.” The following standard electronic transactions are specified by the Security Rule and trigger the need for compliance:

- Health care claims
- Health care payment and remittance advice
- Coordination of benefits
- Health care claim status, enrollment or disenrollment in a health plan
- Eligibility for a health plan
- Health plan premium payments
- Referral certification and authorization
- First report of injury
- Health claims attachments

What are the penalties for non-compliance? The Security Rule is enforced by the Center for Medicare and Medicaid Services (CMS) within the U.S. Department of Health and Human Services, which may impose the following:

- Administrative Action (i.e., implement a corrective action plan created by CMS)
- Civil Penalties ranging from $100 to $25,000
- Fines of up to $250,000 and imprisonment for up to 10 years

The Bottom Line

It makes sense for practitioners who electronically store, access, send or receive patient or patient-related information to ensure they are in compliance with the HIPAA Security Rule. The APA Practice Organization has developed the HIPAA Security Rule Primer and the HIPAA Security Rule Online Compliance Workbook, created especially for practicing psychologists and available at APAPractice.org.

Are you prepared for a Medicare audit?

Psychologists who provide services to Medicare beneficiaries need to be prepared for the possibility of an audit. It’s helpful to know what triggers Medicare audits, how to prevent them, and how to handle an unfavorable audit determination. To read a question-and-answer guide about Medicare audits, visit APAPractice.org.