

# HIPAA Security Rule: Are You Getting Ready?

by Legal & Regulatory Affairs Staff

November 9, 2004 -- The following questions and answers provide some basic information for psychologists about the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. This rule is one of three main rules – in addition to the Privacy Rule and Transaction Rule – affecting psychologists that resulted from HIPAA.

Now is a good time to begin familiarizing yourself with the Security Rule and its requirements. Practitioners need to comply with this rule by April 20, 2005.

## **Q: What is the HIPAA Security Rule?**

**A:** The Security Rule sets standards for administrative, physical, and technological safeguards — such as access to offices, computers and files — needed to keep electronic health care information confidential and secure. It is a companion to the HIPAA Privacy Rule.

While the Privacy Rule outlines to whom and under what circumstances a psychologist can *intentionally* disclose patient information, the Security Rule focuses on protecting information from *unintended* disclosures through breaches of security. This includes any reasonably anticipated threats or hazards and/or an inappropriate uses and disclosures of electronic confidential information.

## **Q: What does the rule cover?**

**A:** The Security Rule, like the Privacy Rule, applies when a covered entity – including a psychologist – transmits information in electronic form in connection with a standard transaction (see the following question). In effect, a psychologist must comply with the Security Rule if having determined previously that he or she is required to comply with the Privacy Rule.

However, there is an important difference between the two rules. Unlike the Privacy Rule, which applies to all 'protected health information' (PHI), the Security Rule applies only to '**electronic protected health information' (EPHI)**.

PHI is defined as individually identifiable health information that is transmitted or maintained in all mediums -- including electronic, written, and oral. EPHI is PHI that is transmitted or maintained in electronic media only.

## **Q: What triggers the HIPAA Security Rule?**

**A:** The following electronic transactions trigger the Security Rule:

- 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

The Security Rule applies when a psychologist – or an entity, such as a billing service, acting on behalf of the psychologist -- transmits health care information in electronic form in connection with any of the transactions listed above. Once a trigger occurs, the Security Rule then applies to all EPHI within a psychologist's practice.

**Q: What steps will the Security Rule require me to take?**

**A:** The first step in the compliance process involves the psychologist doing a "risk analysis" of his or her practice. This analysis is a thorough assessment of the practice's potential security risks and vulnerabilities related to EPHI. The analysis entails reviewing the practice's established security policies and procedures, and it provides the basis for making any appropriate modifications or enhancements to these procedures.

The Security Rule requires health care providers to take steps to ensure:

- The confidentiality of EPHI
- The integrity of EPHI, i.e., making sure the information is not changed or altered in storage or transmission
- The availability of EPHI, i.e., ensuring the information is accessible to the appropriate people when needed

**Q: Does the size of my practice affect my compliance with the Security Rule?**

**A:** Yes. As with the Privacy Rule, the Security Rule embodies the concept of "scalability." This means, for example, that a solo practitioner will not be expected to take the same steps to comply as will a large practice or a health care facility. According to the federal Centers for Medicare and Medicaid Services (CMS), a covered entity such as a health care provider can consider its size, capabilities, and costs in determining what security measures to use.

**Q: Who enforces the Security Rule and what are the potential penalties for non-compliance?**

**A:** CMS is responsible for enforcing the Security Rule. The potential penalties range from administrative action to substantial fines and imprisonment, depending on the severity of the violation.

**Q: What information is available from the APA Practice Organization?**

**A:** The Practice Organization is developing informational materials and products tailored for practicing psychologists, including a primer about the Security Rule. In addition, future issues of this e-newsletter will contain more information about the rule.

You also can link to information available at [APApractice.org](http://APApractice.org) about the HIPAA [Privacy Rule](#) and [Transaction Rule](#).