AMERICAN
PSYCHOLOGICAL
ASSOCIATION
PRACTICE ORGANIZATION

Practice *Working for You*

The HIPAA Security Rule Primer

Compliance Date: April 20, 2005

Printer-friendly PDF

Contents

Click on any title below to jump to that page.

1 What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) resulted from a bill sponsored by Senators Nancy Kassebaum (R-KS) and Edward Kennedy (D-MA). HIPAA was signed into law in 1996.

The HIPAA law was designed to protect Americans who were previously ill from losing their health insurance when they changed jobs or residences. In creating the law, Congress also sought to streamline the health care system by adopting consistent standards for transmitting electronic health care claims in a uniform manner. During the creation of this Administrative Simplification process, Congress also realized the importance of protecting the privacy of an individual's health-related information and securing the storage of such information.

To date, there are **three main rules** that outline HIPAA's implementation requirements:

1. The **Privacy Rule** focuses on when and to whom confidential patient information can be disclosed[1] (compliance date: April 14, 2003).
2. The **Transaction Rule** addresses technical aspects of the electronic health care transaction process and requires the use of standardized formats whenever health care transactions, such as claims, are sent or received electronically (compliance date: October 16, 2003).
3. The **Security Rule** seeks to assure the security of confidential electronic patient information. For psychologists, this usually means addressing administrative, physical and technical procedures such as access to offices, files and computers, as well as the processes a psychologist uses to keep electronic health information secure (compliance date: April 20, 2005).

Understanding the HIPAA rules, and taking the necessary steps to comply with them, may appear daunting at the outset. However, for most psychologists, especially those working independently in private practice, becoming HIPAA-compliant is a manageable process.

This Primer will provide you with a preliminary overview of the HIPAA Security Rule. More detailed tools and information will be available in early 2005.

[1]For a complete analysis of the HIPAA Privacy Rule, see the *HIPAA for Psychologists* product and other materials at www.apapractice.org.

2 What is the HIPAA Security Rule?

While the Privacy Rule outlined to whom and under what circumstances a psychologist can disclose patient information, **the Security Rule outlines the steps a psychologist must take to protect confidential information from *unintended* disclosure through breaches of security.** This includes any reasonably anticipated threats or hazards, such as a computer virus, and/or any inappropriate uses and disclosures of electronic confidential information (for example, confidential patient information e-mailed to the wrong person due to human or technical error). The Security Rule creates standards that health care professionals must meet to keep electronic health care information confidential and secure.

3 In what circumstances does the Security Rule apply?

The Security Rule applies to the following covered entities:

Covered Entity	Health care provider (i.e., psychologist)
	Health plan (including employer-sponsored group health plans, Medicaid, Medicare, etc.)
	Health care clearinghouse[2]

Like the Privacy Rule, the Security Rule applies when a psychologist transmits information in electronic form in connection with a standard transaction (see Triggers on the next page).

The Security Rule sets administrative, technical and physical standards to prevent breaches of confidentiality. One distinction to note is that whereas the Privacy Rule applies to all Protected Health Information (PHI)[3], **the Security Rule applies only to electronically transmitted or stored protected health information (EPHI)**.

[2] **Health care clearinghouse:** A public or private entity that: (a) converts or assists with the process of converting health information into standardized HIPAA-compliant data or a standard transaction; and/or (b) receives a standard transaction and converts or assists with the process of converting that standard transaction back into a non-standard format or non-standard data for the receiving entity.

[3] The Privacy Rule applies to electronic, written and oral PHI.

As you may recall, "PHI" is defined as individually identifiable health information[4] that is transmitted or maintained any form or medium. EPHI is PHI that is transmitted or maintained in *electronic* media. **This means that paper PHI is *not covered* by the Security Rule.**

Triggers

As noted above, the Security Rule applies when a psychologist (or an entity acting on behalf of a psychologist, such as a billing service) transmits information in electronic form in connection with a transaction specified by the Rule. Once a trigger occurs, the Security Rule then applies to all EPHI within a psychologist's practice.[5]

The following **standard electronic transactions** are specified by the Security Rule and trigger the need to be HIPAA-compliant:

- 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

Electronic Transmission

The mode of electronic transmission includes the Internet, extranets (using Internet technology to link a business with information only accessible to collaborating parties), dial-up lines, computer-generated faxes (not traditional paper-to-paper faxes), private networks, and EPHI that is physically moved from one location to another using magnetic tape, disk or compact disc media.

---

[4] **Individually identifiable health information:** Information that is a subset of health information that either identifies the individual or that can be used to identify the individual. Health information: Any information, whether oral or recorded in any form, created or used by health care professionals or health care entities.

[5] The Privacy Rule is triggered in the same way as the Security Rule. Thus, if you trigger one rule, you trigger both rules and need to comply with both.

4 How will the Security Rule affect your practice?

The Security Rule requires that steps be taken to ensure:

- The confidentiality of EPHI;
- The integrity of EPHI (meaning the information is not changed or altered in storage or transmission); and
- The availability of EPHI (making sure the information is accessible to the appropriate people when needed).

Complying with the Security Rule is a process that begins with a **risk analysis**. The risk analysis is a careful and thorough documented evaluation of whether your practice's administrative activities, physical environment and computer systems are secure, and whether EPHI is accessible only to appropriate and authorized individuals.

The risk analysis will help you to determine and document any security threats or vulnerabilities (e.g., floods, computer viruses, or break-ins) in your practice by comparing current activities with the administrative, physical, and technological requirements of the Security Rule. As part of the risk analysis process, you will also assess the *likelihood* and *impact* of identified threats and vulnerabilities and take any necessary preventive and corrective actions to bring your practice into compliance in the event of a breach of security.

Each stage of the risk analysis must be documented and the completed risk analysis document added to your HIPAA compliance records. You will also need to update relevant Policy and Procedure documents[6] to reflect any administrative, physical, or technical safeguards that have been implemented as a result of the risk analysis.[7]

If you are operating in a setting (such as a large facility) that currently has a HIPAA Security Officer responsible for implementation and compliance, you should defer to that individual's guidance on how to comply with the Security Rule, even when the Security Officer's guidance differs from this Primer.

---

[6] Because written policies and procedures are required as part of prior HIPAA Privacy Rule compliance activities, this document assumes that all HIPAA-compliant psychology practices have written HIPAA-related Policies and Procedures guiding their daily operation. Psychologists interested in learning more about Privacy Rule compliance should visit www.apapractice.org for more information. The APA Practice Organization and the APA Insurance Trust have also teamed up to bring you *HIPAA for Psychologists*, the most comprehensive resource available to help you comply with the HIPAA Privacy Rule. *HIPAA for Psychologists* – also available at www.apapractice.org – provides information about the Privacy Rule and the customizable, state-specific forms needed to be compliant.

[7] As you work through your risk analysis, you may notice that you have already complied with certain Security Rule standards in your efforts to comply with the Privacy Rule (e.g., the Privacy Rule requires that HIPAA-compliant psychologists implement reasonable safeguards to protect an individual's privacy).

5 How is the Security Rule organized?

The Security Rule contains specific Standards that give direction on how to meet the Rule's requirements.

The Standards

The **Standards** are organized into three categories:

1	2	3
Administrative Standards	**Physical Standards**	**Technical Standards**
address the implementation of office policies and procedures, staff training, and other measures designed to carry out security requirements.	relate to limiting access to the physical area in which electronic information systems are housed.	concern authentication, transmission and other issues that may arise when authorized personnel access EPHI via computer or other electronic device.

Accompanying these Standards are Implementation Specifications that provide specific details on how to implement the Standards. (The Standards are defined in detail starting on page 11.)

Although the Standards are divided into three categories, there is overlap in terms of content and compliance activities. As a result, compliance may be achieved through one or possibly a series of actions depending on the size and complexity of your practice.

For example, one of the Physical Standards states that a psychologist should put physical safeguards in place to protect against unauthorized access to a psychologist's computer. If the computer is located in a locked office and can only be accessed by authorized employees, the psychologist may have met this standard (depending on other factors such as locale, i.e., high crime area). This Physical Standard overlaps with the Administrative Standard which states that only appropriate personnel should have access to EPHI. In a small practice, where only appropriate personnel have keys to the door locks, complying with the Physical Standard (e.g., locking the office) may also meet the Administrative Standard. In a larger practice, where employees have office keys but not all should have access to the computer network, compliance may also require the development of an administrative policy that outlines procedures to limit access to the computer network (which may include technical aspects such as passwords).

A further overlap also occurs in one of the Technical Standards, which requires procedures to verify the identity of individuals seeking access to EPHI. Again, in a small practice, compliance with the Physical Standard may also meet this Standard, because only employees with keys to the office can access the computer. However, compliance for a larger practice might require an administrative and technological

solution, such as creating a process for assigning employees computer passwords and electronically recording the identity, date and time that a particular employee accessed the computer network.

So depending on the size and complexity of your practice, being in compliance with the Security Rule could mean that EPHI can only be accessed by authorized personnel with personalized passwords, and that the entire system is located behind locked doors accessible only by authorized employees.

Although it may seem redundant to have all three of these Standards in place, the three collectively create a safety net for guarding against inappropriate disclosure of EPHI.

Implementation Specifications

Implementation Specifications provide more specific guidance to help determine which tasks should be undertaken to comply with each Standard. Not every Standard has an Implementation Specification, but some Standards have several. Standards that do not have Implementation Specifications are not optional, and psychologists will need to take reasonable efforts to comply.

Each psychologist's practice is unique and could achieve compliance in several different ways. To communicate a sense of the range of options, Section 6 of this Primer contains examples of Implementation Specifications for each of the Standards.

All of the Implementation Specifications can be found in the Rule itself:
http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp.

Required vs. Addressable

Because HIPAA applies to a wide range of entities, from solo practitioners to health care systems, a concept is applied to attempt to make the process work for all parties. This concept categorizes an Implementation Specification as either "required" or "addressable." If a specification is considered basic to implementing the Standards of the Rule, it is termed "required" and must be implemented. If it is termed "addressable," a psychologist has more latitude to tailor implementation of a Standard to his or her individual practice or, in some instances, to dispense with the Implementation Specification altogether. According to the Rule, if the Implementation Specification is addressable, the psychologist can:

> Assess whether an Implementation Specification is reasonable and an appropriate safeguard for the particular kind of practice; and then:

1. Choose to implement it as it is;
2. Choose to implement an equivalent measure, if reasonable and appropriate; or
3. Choose not to implement it, provided a reasonable rationale exists for not doing so.

Whatever choice is made must be documented, along with a rationale based on risk analysis, particularly if it is an equivalent measure or no measure at all.

For example, under the Security Awareness and Training Standard there is an addressable Implementation Specification that states that Security Reminders (i.e., bulletins, e-mails) should be sent to staff about potential security threats. If a psychologist has performed a risk analysis of his or her solo practice, he or she may determine that there is no need to implement this Implementation Specification because he or she does not employ any staff.

Scalability

Scalability is another concept that was created as part of the Security Rule to tailor the process to the size and complexity of one's practice. When considering what steps must be taken to comply with the Security Rule, a psychologist should take the following aspects of his/her practice into account to determine to what degree one must comply:

- Size
- Complexity
- Capabilities
- Technical infrastructure
- Cost of procedure to comply
- Potential security risks

For example, the Security Rule requires the psychologist to designate a HIPAA Security Officer. For a solo practitioner, it would be unduly expensive to hire someone to fill this role, and doing so would not make sense in light of the relatively limited complexity of his/her security issues. Accordingly, it would be appropriate for the solo practitioner to simply designate himself/herself as the Security Officer.

6 The Standards

Below is a detailed overview of each of the three categories of Standards – Administrative, Physical and Technical – along with examples of Implementation Specifications.

Administrative Standards

Administrative Standards relate to the administrative actions that a psychologist must take to train staff, or to what administrative activities the psychologist must take, to carry out security requirements. This includes implementing current office policies and procedures for ways to prevent, detect, contain, and correct security violations.

The Administrative Standards are as follows:

1. **Assigned Security Responsibility:** Appoint a HIPAA Security Officer who will be responsible for developing and implementing security policies and procedures for your practice (e.g., in a solo practice, the psychologist would typically be the HIPAA Security Officer).

2. **Security Management Process:** This standard requires the HIPAA Security Officer (in a solo practice, this could be the psychologist, as previously noted) to create and implement policies and procedures that are designed to prevent, detect, contain, and correct HIPAA security violations (e.g., the HIPAA Security Officer could create a policy that requires all employees to report breaches of security policies by fellow employees).

3. **Workforce Security:** Implement policies and procedures to ensure that all employees have appropriate access to EPHI. Also ensure that those employees who should not have access are unable to access EPHI (e.g., a policy could be created that requires an appropriate screening of each potential employee and verification of each reference prior to hiring).

4. **Information Access Management:** Implement policies and procedures that authorize your employees' access to EPHI (e.g., a policy could be created to monitor access to EPHI by limiting access to certain employees with specific passwords).

5. **Security Awareness and Training:** Implement a security awareness and training program for all members of your workforce (e.g., a tutorial given by the psychologist on how to protect EPHI).

6. **Security Incident Procedures:** Implement policies and procedures to address breaches of security (e.g., if an employee inadvertently leaves EPHI visible on a computer screen, retraining on security procedures may be warranted).

7. **Contingency Plan:** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrences that threaten the security of electronic records (e.g., fire, vandalism, system failure, and natural disaster).

8. **Evaluation:** A psychologist should regularly evaluate his or her technical (computer) and non-technical systems to ensure that EPHI is adequately protected, especially if the psychologist has recently updated his or her risk analysis.[8] This evaluation should also explain how the psychologist's policies and procedures comply with the Security Rule requirements.

9. **Business Associate Contracts:** Initiate policies and procedures to ensure that all business associates are in compliance with the Security Rule (e.g., provisions built into a contract with a billing service).

Implementation Specifications for Administrative Standards (examples)

As mentioned, along with the Standards are Implementation Specifications, which give further details for implementing the Standards. In the Administrative Standard category, there are twenty-one (21) Implementation Specifications. Ten (10) are required, and eleven (11) are addressable. Examples of each are given below:

Sanction Policy (Required):

This Implementation Specification is a requirement of the Security Management Process Safeguard Standard (Standard 2, see page 11). In this Specification, a psychologist is required to implement a sanction policy that clearly delineates consequences for violations of security policies and procedures by employees, agents, and contractors. Consequences could include retraining the employee who violated the policies and procedures, or perhaps terminating the individual if the violation is egregious.

Sanctions must be applied equally to all individuals, and the policy should apply to any and all violations. If a psychologist has complied with the Privacy Rule, a Privacy Rule sanction policy should already be in place. This policy could be modified to address both Privacy and Security Rule requirements.

Workforce Clearance Procedures (Addressable):

Workforce clearance procedures are an addressable Implementation Specification under the Workforce Security Standard. This Specification ensures that individuals who have access to EPHI have been given appropriate clearance. An example of a workforce clearance procedure might be a background check for employees who deal with EPHI.

[8] The Security Rule requires periodic updates of a psychologist's risk analysis to ensure ongoing compliance. More detail on this topic is discussed later in this document.

Because this Specification is addressable, you can assess your practice and determine if compliance can be accomplished in reasonable manner. For example, if the only employee in your practice is yourself, you would not need to undertake a clearance procedure on yourself (the specification does not apply). You would, however need to document why the Specification does not apply (e.g., the only employee is yourself). In a small practice with only a few employees, a reasonable effort to meet this Specification might be calling a prospective employee's references and asking about their reliability and trustworthiness. In a larger organization, addressing this Specification by requiring formal background checks (e.g., criminal record, bankruptcy, etc.) may be what is necessary to be considered compliant and reasonable.

Business Associates Contract (Required):

This Implementation Specification requires a psychologist to obtain "satisfactory assurances," in the form of a contract or agreement from his or her business associates, that the associate will comply with the Security Rule requirements. This contract or agreement can be combined with a psychologist's current Privacy Rule business associates contract or agreement.

Physical Standards

Physical Standards require psychologists to implement policies and procedures that limit physical access to electronic information systems (e.g., computers) and the facilities (e.g., a business office) in which the electronic records are housed. Examples might be as simple as a lock on the door of the room in which the computers are located or as complex as a retinal scan.

The Physical Standards are as follows:

1. **Facility Access Controls:** Mechanisms must be in place to ensure that only authorized staff can enter the office suite and remove systems or media containing EPHI (e.g., a log could be created that identifies which employee has keys to the office and also notes when the key has been returned).

2. **Workstation Use:** Implement policies and procedures that describe appropriate functions for a specific workstation (for example, a cubicle) or class of workstations that are used to access EPHI (for example, restricting the EPHI available on a reception area computer to only the EPHI needed to schedule or change an appointment).

3. **Workstation Security:** Mechanisms must be in place to ensure that computer workstations and all other devices are secure and used appropriately (e.g., securing the computer to a desk, with screens turned so they cannot be seen by casual observers).

4. **Device and Media Controls:** Implement policies and procedures that ensure security when a psychologist is moving computers and/or other electronic media (e.g., floppy disks, backup tapes, etc.) that contain EPHI within and outside of his or her facility (e.g., remove all sensitive information from the computer before transferring the computer to another user).

Implementation Specifications for Physical Standards (examples)

In the Physical Standards category, there are eight (8) Implementation Specifications. Two (2) are required, and six (6) are addressable. Examples are given below.

Media Reuse (Required):

This Implementation Specification requires a psychologist to assure that all storage media containing EPHI (i.e., diskettes, CDs and DVDs) are carefully cleansed of all data and images prior to reuse. This cleansing could be achieved with a number of software programs (e.g., a disk wiper could be used to remove the data).

Contingency Operations (Addressable):

Contingency Operations are an addressable Implementation Specification that need only be implemented if necessary. This Implementation Specification could be addressed by establishing procedures that allow the psychologist and personnel to access EPHI in a disaster or in emergency situations. For example, a special process could be created that would allow certain individuals to retrieve backup data and transfer that data to a different computer system in emergency circumstances such as a hurricane or electrical storm.

A psychologist may not have to implement this Implementation Specification if he or she has covered this security concern through compliance with another Implementation Specification (e.g., a technical measure that automatically backs up critical EPHI to a remote computer) or if the psychologist's risk analysis has determined that this is not a significant risk. However, it would not be adequate to simply state it is not a risk; one should explain and document why this is so.

Technical Standards

Technical standards require a psychologist to create policies and procedures that govern the technical aspects of accessing EPHI within computer systems by appropriate persons (e.g., computer passwords and encryption software).

The Technical Standards are as follows:

1. **Access Controls:** Implement technical policies and procedures for computers to ensure only appropriate access to EPHI by authorized individuals (e.g., issuing individual passwords).

2. **Audit Controls:** Implement hardware, software, and/or procedural mechanisms that monitor EPHI for security breaches (e.g., creating a log that shows who accessed a particular computer and when).

3. **Integrity:** Implement policies and procedures to protect EPHI from improper alteration or destruction (e.g., regularly updating and running anti-virus and firewall software).

4. **Person or Entity Authentication:** Implement procedures to verify that a person or entity seeking access to EPHI is the one claimed (e.g., using and regularly changing individual passwords).

5. **Transmission Security:** Implement technical security measures to guard against access to EPHI that is being transmitted over an electronic communications network (e.g., using secure transmission systems or encryption when e-mailing or transmitting patient data).

Implementation Specifications for Technical Standards (examples)

In the Technical Standards category, there are seven (7) Implementation Specifications. Two (2) Specifications are required, and five (5) are addressable. Examples are given below.

Unique User Identification (Required):

A Unique User Identification is a required Implementation Specification. This means that every individual in the workplace must have his or her own unique name and/or number for access to the computer system. *Sharing user identifications is no longer permitted.* In a solo practice, this required Standard might have no practical effect, but in a larger practice a stringent enforcement policy may be required to assist the workforce with observing this required specification.

Encryption and Decryption (Addressable):

This addressable Implementation Specification provides for the implementation of a mechanism to encrypt and decrypt EPHI. In a larger practice, with established policies and procedures for sharing encryption "keys" with authorized entities, purchasing a computer program that encrypts and decrypts data may be an appropriate way to address this Implementation Specification. Because this is addressable, a small practice may choose to use a HIPAA-compliant secure messaging service, which meets the security goal of this Implementation Specification without requiring a psychologist to obtain encryption software.

7 Compliance Documentation

For all Standards and Implementation Specifications, the covered entity (e.g., a psychologist) must maintain a policies and procedures document in written or electronic form that explains how he or she has complied with each step of implementation.

Compliance with the HIPAA Security Rule requires that a psychologist undertake *a process* by which he or she analyzes and documents each step that has been taken to become compliant. That means that for all Security Rule Standards and Implementation Specifications, psychologists must develop and maintain a policies and procedures document in written or electronic form, that explains how he or she has complied with each step of implementation.

This document must be retained for six (6) years from either the date it was created or the date it last went into effect, whichever is later, and the document must be made available to those persons responsible for implementing the procedures. These Policies and Procedures must be promptly updated to comply with any changes in the law or any changes in how you plan to comply with the Standards.

8 Government Enforcement and Penalties

The Security Rule is enforced by the Center for Medicaid and Medicare Sciences (CMS). The following **actions and/or fines** could be based upon a Security Rule violation:

- 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 ten (10) years

These same penalties can be imposed for Privacy Rule violations; however, the Privacy Rule is enforced by the Office of Civil Rights (OCR).

9 What's next?

The Practice Organization is developing a comprehensive, easy-to-use tool to assist psychologists with Security Rule compliance and documentation processes, step by step. More information about this tool will be available shortly.

In keeping with HIPAA's focus on administrative simplification, CMS will shortly be providing information about how the HIPAA National Provider Identification (NPI) Rule will be implemented. The NPI rule is designed to create an identification number unique to each covered entity (e.g., psychologist) for use in all standardized transactions. Covered entities may begin obtaining NPIs on March 23, 2005, and all covered entities are required to have obtained an NPI by March 23, 2007. As psychologists begin implementing Security Rule policy, this will be a good time to consider the need to obtain an NPI. More information about the NPI will also be available shortly.

Regular updates on HIPAA are available at www.apapractice.org. Should you have additional questions after visiting www.apapractice.org, please contact the APA Practice Organization's Legal and Regulatory Affairs Office at (202) 336-5886.