

This article summarizes a primer, "Getting Ready for HIPAA: What You Need to Know," written by the APA Practice Organization and the APA Insurance Trust. All APA Special Assessment members should already have received this primer. If you read APA's primer, and this article, you will understand HIPAA's basic requirements and have the information necessary to begin to comply with this new federal law.

**There is no out.
There are no exclusions.
All psychologists must
make their practice
HIPAA compliant.**

The Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) was sponsored by Senators Nancy Kassenbaum and Ted Kennedy and signed into law on August 21, 1996. The goal of this bill was essentially twofold: first, to make insurance more portable by ensuring that individuals would not lose their insurance coverage when they changed jobs and by promoting the simplification of health care administration by creating a uniform electronic transactions process. The intent of the second goal is significant dollar savings through the adoption of uniform electronic claims transmission standards.

It soon became obvious that strict privacy and security standards would have to be developed to protect the health care information that would be transmitted electronically.

The APA Practice Organization (formerly the Practice Directorate), in partnership with the APA Insurance Trust (APAIT), will continue to provide you with information necessary to comply with HIPAA. APA's Practice Organization has devoted considerable resources to helping psychologists with this task. For example, they are in the process of developing the necessary forms and templates to help you in your practice. MPA will help with additional resources and materials.

HIPAA included a provision that required Congress to develop privacy standards. According to the statute, if Congress was unable to enact privacy standards by August 21, 1999 then the Secretary of Health and Human Services was required to develop the privacy regulations. Congress did not meet the guidelines, and, as a result, HHS developed the privacy rules. These rules became effective on April 14, 2001 with a required compliance date of April 14, 2003. Small health plans will have until April 14, 2004 to comply with the rule.

The Nuts and Bolts of HIPAA

HIPAA contains three rules

1. The Privacy Rule
2. The Transaction Rule
3. The Security Rule

This article focuses on the Privacy Rule since we will be most concerned with and affected by that particular Rule. A second Rule, the Transaction Rule, requires standard formatting for all electronic transactions and will be handled by insurance companies, claims clearing-houses, billing companies, and your own billing software.

The Transaction Rule was finalized in October 1999 with an initial compliance date of October 2002. This compliance date will be extended to October 2003 for everyone who submits an extension form to HHS by October 16, 2002. The form has been developed by HHS, is available on their website—www.cms.gov/hipaa/hipaa2/ASCAForm.asp., and must be submitted by the October 16, 2002 deadline. Individu-

als who do not submit the extension form will be required to comply with the Transaction Rule by October 16, 2002. Therefore, everyone should submit the extension form.

HIPAA does not require electronic claims submission. However, most people expect that insurance companies will require electronic claims submission at some point in the future. The Transaction Rule is only one of the three HIPAA rules (Privacy Rule, Security Rule, Transaction Rule) and even if you never submit bills electronically you will still need to comply with HIPAA's Privacy and Security Rules

The Security Rule has not yet been finalized although we know that the proposed Rule addresses required standards for our physical infra-structure (e.g., access to offices, files, computers) to ensure secure and private communication. This should not be a significant burden to psychologists since we have consistently held ourselves to a high standard regarding the communication and maintenance of confidential patient information.

Early drafts of the Security Rule

suggest that the following will be required:

- **Contingency Planning** – development of a formal process to analyze and inventory the types of data that are stored electronically and how the integrity of that data will be protected in the event of an emergency, disaster, or theft;
- **Information Access controls** – define who has access to PHI, the rules determining a person's right of access, and the reason for denying access to some individuals;
- **Staff Training** – provide staff members with training and education about handling PHI;
- **Physical Safeguards** – maintain "reasonable and appropriate" policies and procedures for the physical security of PHI. Typically, this would involve records storage areas, fax machines, and computer workstations;
- **Technical Security** – Passwords, identification, digital signatures, firewalls, virus protection and encryption are standard measures to protect the privacy and integrity of information flowing within and between computer networks.

Who Is Covered by HIPAA?

All psychologists and their practices must comply with HIPAA's requirements. As will be obvious from the rest of the article, the only way to avoid triggering HIPAA is the following: you have no telephone, have no computers, have no fax machine, don't have any medical records, and don't see any patients. Therefore: ***There is no out. There are no exclusions. All psychologists must make their practice HIPAA compliant.*** However, this is not as daunting a task as it may seem. The American Psychological Association's Practice Organization, the APA Insurance Trust, and the Maryland Psychological Association are working to develop the necessary forms and templates to help you in your practice. Your task is not complicated and will not be especially onerous:

1. Read articles sent to you by the American Psychological Association's Practice Organization and the APA Trust;
2. Read articles in the Maryland Psychologist; and
3. Follow the suggestions outlined in those articles.

What are the consequences of failing to comply with HIPAA?

The Health and Human Services Office for Civil Rights will monitor compliance. Their first goal is education, not civil and criminal penalties. But penalties may be assessed after an initial period of education. Civil penalties will not be more than \$100 for each violation not to exceed \$25,000 in a calendar year, all the way up to fines of up to \$250,000, imprisonment for up to ten years, or both.

HIPPA's Privacy Rule

The majority of our work will focus on ensuring compliance with HIPAA's Privacy Rule. The Department of Health and Human Services (HHS) published the final Rule (65 FR 824682) on December 28, 2000, establishing "Standards for Privacy of Individually Identifiable Health Information" ("Privacy Rule"). After a lengthy public comment period, the Secretary of HHS decided that the Privacy Rule would stand as published and become effective on April 14, 2001.

The Department of Health and Human Services, however, proposed some modifications to the Privacy Rule on March 27, 2002. The thirty-day comment period has passed and the Department is expected to finalize modifications in the immediate future. Specific proposed modifications are outlined at the end of this article.

In broad terms, the rule will require us to:

- Develop policies and procedures regarding patients' privacy rights, employee training to ensure their understanding of privacy procedures, and protection of patient records;
- Put into place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information;
- Provide consent forms and information forms to our patients concerning their privacy rights;
- Maintain documentation of consents, authorizations, procedures and policies, training, and other activities undertaken in compliance with the Privacy Rule;
- Designate a "privacy officer" who will be responsible for ensuring that privacy procedures are adopted and followed (in small practices, this can be the psychologist or an appropriate staff person); and
- Designate a contact person, whom people can contact with questions about privacy.

The HIPAA Privacy Rule applies to "covered entities" which includes:

- Health Care Providers (includes any person or entity that furnishes, bills, or is paid for health care services in the normal course of business. "Healthcare" is defined as "care, services, or supplies related to the health of an individual.")
- Health Plans (includes employer sponsored group plans, Medicaid, Medicare, etc.)
- Health Care Clearinghouses (an entity that translates health information received from other entities either into or from the standard format that will be required for HIPAA transactions)

HIPAA requires that the Privacy Rule be "scalable." "Scalable Compliance" means that a covered entity must "reasonably" meet the requirements according to their size and type of activities. This is written right into the Privacy Rule because HHS recognized that individual practitioners and small practices do not have the resources available to a larger practice or hospital.

The HIPAA Privacy Rule sets a floor for protection, not a ceiling, and was designed to serve as a minimum level of privacy protection. Therefore, any state law that provides greater protection for patients will supercede HIPAA. This will require a side-by-side analysis of state law and HIPAA to determine which law we follow – HIPAA or Maryland State Law. This analysis will be done by APA and MPA and distributed to MPA members.

The Privacy Rule applies to "Protected Health Information (PHI)." Protected Health Information is defined as patient information that identifies the individual or can be used to identify the individual, and is transmitted or maintained in any form or media. Specifically, PHI is "information which relates to the past, present, or future physical or mental health condition of an individual; provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and, that identifies the individual or could reasonably be used to identify the individual."

The Privacy Rule is triggered under specific circumstances. Expert analysis reveals that no psychologist will be able to escape a trigger. Therefore, as stated at the very beginning, all psychologists must become HIPAA compliant. Specifically, the Privacy Rule is triggered when the following occurs (but is not limited to the following):

- A patient submits a bill to an insurance company for reimbursement
- A psychologist transmits protected health information in an electronic form in connection with:
 - Health care claims and payments
 - Coordination of benefits
 - Health care eligibility, claims status, enrollment, or disenrollment
 - Referral certification and authorization
 - First report of injury
 - Health claims attachments
- When an entity acting on behalf of the psychologist transmits PHI in electronic form (e.g., billing service).

"Transmitting in electronic form" includes:

- Transmissions using the Internet, extranet (using internet technology to link a business with information only accessible to collaborating parties)
- Using lease lines, dial-up lines, private networks
- Transmissions that are physically moved from one location to another using magnetic tape, discs, or compact discs medium

Remember that The Privacy Rule is triggered as soon as protected health information is transmitted electronically, which includes being stored electronically. Therefore, even leaving a message on a telephone answering system could be a trigger for the Privacy Rule. While the telephone is not considered to be an electronic medium, it is likely that when you leave messages on a voice mail system that the information is being stored electronically. This will trigger HIPAA. Similarly, use of a fax machine must be treated as if the Privacy Rule applies. For example, even if you use paper at your end of the fax transmission (you put a piece of paper in your fax machine), the fax at the other end may be accepted in electronic form, thus triggering HIPAA. Similarly, when you receive a fax, there is no way to know whether the information was stored or sent electronically (e.g., from a computer equipped with fax software and a modem), thus triggering the Privacy Rule.

Some General Provisions Under the Privacy Rule

The Privacy Rule differentiates consent and authorization. Consent is a bottom line threshold that is required before we can even provide treatment to our patients. Consent forms generally advise patients that their health information may be used for treatment, payment and health care operations purposes and inform them of their general rights with respect to this information. The consent form must state that the individual has the right to revoke the consent in writing. Consents do not contain specific details of the covered entities use and disclosure of health information, but refer patients to the entities' notice of privacy practices for that information.

- "Treatment" includes: Providing health care to a patient; coordinating and/or managing a patient's care with a third party; consulting with another provider; and, referring a patient to another provider.
- "Payment" includes: obtaining reimbursement for the provision of health care, billing, claims management, health care data processing, and other activities.
- "Health care operations" includes: quality assessment (e.g., outcomes evaluation); case management and care coordination; peer review; accreditation and licensing; conducting or arranging for medical review, legal services, and auditing functions; customer services; business management; and, other activities.

Authorization is a more specific level of protection than the general consent. Authorization is similar to what we think of as a standard release of information form. The Privacy Rule requires that we obtain patient authorization when we release protected health information for purposes other than treatment, payment, or health care operations. This would include, for example, the release of PHI to an employer or school.

Patient authorization must include the following:

- A specific definition of the information to be used or disclosed;
- To whom the information is going to be disclosed;
- The purpose of the disclosures;
- An expiration date;
- The right to revoke the authorization; and,
- The right not to authorize the disclosure.

Neither consent nor authorization is required for use and

disclosure in several specific circumstances including:

- To show compliance with the Privacy Rule
- For health oversight activities of the originator of Psychotherapy Notes (defined below)
- To a coroner or medical examiner for identification, cause of death, or other duties authorized by law (this will be subject to state preemption)
- To avert a serious threat to the health or safety of a person or the public
- The military, veteran's affairs, or another entity for national security purposes
- A hospital or other type of facility for their facility directory
- Worker's Compensation laws
- Victims of abuse, neglect, and domestic violence
- Other situations as required by law.

"Psychotherapy Notes" are specifically defined in HIPAA and are treated differently than the rest of the patient's medical record. Psychotherapy notes require a specific authorization before they can be released. The APA Practice Directorate spent many hours advocating on our behalf to ensure that psychotherapy notes would be classified differently than the rest of the medical record and would require a specific authorization for release. Psychotherapy notes are defined as "notes recorded in any medium by a mental health provider documenting or analyzing the contents of a conversation during a private, group, joint or family counseling session, and that are separated from the rest of the individual's medical record." These notes, which we would typically think of as process notes, must be kept in a separate file and segregated from the rest of the medical record.

The definition of "Psychotherapy Notes" excludes: "information pertaining to medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests and any summary of the following items: Diagnosis, Functional status, Treatment plan, Symptoms, Prognosis, Progress to date."

Psychological testing is not included in the definition of psychotherapy notes and can be interpreted to be specifically excluded (e.g., results of clinical tests) and therefore could be released with a general consent as opposed to a more specific authorization.

Minimum Necessary Disclosure

Minimum necessary disclosure refers to the amount of information released when PHI is disclosed or used with a general consent (as opposed to a specific authorization which details the information to be disclosed). The Privacy Rule requires that we release the minimum PHI necessary to respond to the request for information.

HIPAA specifically requires that we release no more information than is necessary to conduct the activity for which the information is requested and to complete the "task at hand." Therefore, when managed care companies or insurance companies request PHI to determine medical necessity, psychologists must only release the minimum information necessary to conduct that specific activity.

At present, there is no hard and fast rule or clear policy as to what is considered to be minimum necessary information.

Therefore, psychologists may find themselves in the position of releasing what they believe to be the information necessary for the managed care company to complete utilization review, but the company may then respond and say they cannot do the task at hand and they require additional information. It is expected that it will take some time to determine what is meant by "minimum necessary disclosure."

HIPAA also specifically states that a covered entity, such as a managed care or insurance company, cannot condition treatment, eligibility for benefits, or payment of claims on a patient's willingness to authorize disclosure of psychotherapy notes — payment cannot be denied because a patient will not authorize release of their psychotherapy notes.

The minimum necessary disclosure does not apply to requests for information that require a specific authorization above and beyond the general consent (such as with psychotherapy notes). This is due to the fact that the information to be disclosed is specifically described by the authorization itself.

State Laws Preemptions

Federal law typically preempts state law. However, this is not the case with HIPAA's Privacy Rules since they are viewed as a floor for patient protection. Therefore, if a state law is more protective from a patient's standpoint, then that state law will preempt HIPAA.

If HIPAA and state law are "contrary" — that is, it is impossible to comply with both state and federal requirements — then it is necessary to do a "preemption analysis" to determine if the state law is stricter and more stringent in its protection of health information. The preemption analysis is always viewed from the consumer's perspective. We must determine which law (state or HIPAA) has more protections for PHI, which has greater requirements for authorization or consent to disclose, which gives greater access to the individual to view their own record or amend their record, which requires higher record keeping standards, and which allows individuals to monitor disclosures of their PHI.

This preemption analysis must be done on a provision-by-provision basis. Therefore, one provision of a State's Privacy Law may preempt HIPAA while others may not.

The federal ERISA (Employment Retirement and Income Security Act) Law further complicates this picture. As you may know, self-funded (aka, self-insured) companies are exempt from state insurance law because of ERISA. (A self-funded company is a large company that does not actually purchase health care insurance for its employees, but, instead, pays for health claims directly from its own checkbook. These employers typically hire insurance companies to process the claims and write the checks so it appears, for all intents and purposes, that the employee actually is covered by an insurance policy.) Companies exempt from state law because they are self-insured would follow a lesser restrictive HIPAA provision as opposed to a more restrictive state law. This means that we will be required to follow different laws for different patients depending upon whether they have insurance or are covered by a self insured company policy.

As always, there are exceptions. Psychologists and other "covered entities" must follow state law in three situations, even if HIPAA is more stringent than state law:

1. When state law provides for the reporting of disease of injury, child abuse, birth or death, or for the conduct

of public health surveillance, investigation or intervention;

2. When state law requires a health plan to report, or to provide access to, information for the purpose of management and financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals;
3. When a Governor requests and has been granted a waiver from the Secretary of HHS because the Governor determined that a particular provision of state law is necessary:
 - To prevent fraud and abuse related to health care;
 - To ensure appropriate regulation of insurance and health plans;
 - For state reporting on health care delivery or costs; and,
 - For purposes of serving a compelling need related to public health, safety, or welfare.

General Consent and Patient's Rights (including access to records)

One of HIPAA's goals is to provide patients with greater access to their records and accurate information regarding the use of their records. As a result, we will be required to provide information about use of the patient's records to patients in a general consent form at the beginning of treatment or, if a patient is continuing in treatment, information about their rights at the time of the implementation of the HIPAA rule.

This consent form is a written agreement between the psychologist and the patient about the potential uses of their PHI and what information will and will not be disclosed. The consent must also include information about their right to limit uses and disclosures. The psychologist must agree to "reasonable requests" for restrictions such as requests that information not be sent to specific individuals.

The provider maintains some discretion regarding patient's requests not to disclose information and this must be detailed in the general consent form. For example, a psychologist can refuse to comply with a patient's request to restrict the release of data if that would result in the psychologist not getting paid for his/her services (e.g., complete a treatment plan, send a HCFA to an insurance

company.) Furthermore, the provider can condition the offering of treatment based on the patient's willingness to release information (e.g., to an insurance company for payment).

The Privacy Rule also creates a right to request that communications be made by specific means or at specific locations and psychologists must agree to "reasonable requests". For instance, a patient could request that bills for health care services be sent to a relative's house, instead of to her home. Providers must accommodate such requests if they are reasonable. The Privacy Rule recognizes that there may be practical consequences to accommodating a request for confidential communications and permits a provider to impose certain conditions on fulfilling such a request (e.g., request must be in writing, provide information about how payment will be handled, provide an alternative address or another method of contact).

Business Associates

A "Business Associate" (e.g., accountant, lawyer, billing service, collection agency) is not a covered entity but performs a service for a covered entity (e.g., the psychologist). Psychologists will be required to have business associates sign a contract that establishes policies regarding use and disclosure of patient records. A business associate's sub-contractors must also agree to all the contract's conditions and restrictions. In effect, therefore, while a business associate is not a covered entity, they will be required to comply with HIPAA as a result of this contract. The psychologist and their business associates must monitor the contracts to ensure that all terms are met. If breached, the psychologist must take reasonable steps to remedy this breach. If those steps aren't successful, the psychologist may have to terminate the contract and/or report the problem to Health and Human Services.

A business associate relationship is not created when the psychologist:

- Furnishes PHI to a postal or courier service
- Discloses PHI to a federal oversight health agency
- Responds to a law enforcement request
- Discloses information within a covered entity (e.g., one's own practice)
- Discloses PHI for treatment purposes (e.g., disclosure by a psychologist to another health care provider for treatment purposes)

HIPAA allows patients to inspect and obtain a copy of their PHI in the "designated record set," defined as the medical and billing records maintained by the provider and used to make decisions about the patient. The psychologist may require that the request be made in writing and in most instances the request must be fulfilled within thirty days. HIPAA does not allow patients access to their Psychotherapy Notes.

Patients have the right to amend their record if they believe the record is incomplete or not accurate. Patients may not expunge any prior information or part of the record; rather, their amendments are part of the patient's ongoing file. Requests for record amendments may be denied if the information is accurate and complete or if the psychologist is not the originator of the information. If an individual, however, provides the psychologist with reasonable basis to believe that the originator of the PHI is no longer available to act on the request, the psychologist must address the request as though he/she created that information.

The patient's record must contain all communication concerning granting and denying requests for record amendments. The record must also contain a listing of all disclosures of PHI for the previous six years. Individuals have a "right of accounting" of all disclosures. The accounting:

- Must be made within sixty days of the request;
- Is provided at no charge one time per twelve month period with a reasonable cost based fee for more than one disclosure per twelve month period; and,
- Must include the following information:
 - The date;
 - Name and address of the entity receiving the PHI;
 - A brief description of what was disclosed;
 - A brief statement of the purpose of the disclosure or, in place of such a statement, a copy of the patient's written authorization.

**For More Information,
Go to
www.marylandpsychology.org**

Summary of DHHS Proposed Modifications to the Privacy Rule (3/27/02)

The Department of Health and Human Services proposed some modifications to the Privacy Rule on March 27, 2002. The following is a brief summary of important proposed modifications:

1. Consent and Notice
 - Applies to used and disclosures for treatment, payment and health care operations purposes (TPO)
 - Patients would acknowledge receipt of the notice of privacy rights and practices, but would not be required to sign a consent form prior to receiving treatment
2. Use and Disclosure
 - A single type of authorization form would be allowed for patient permission for use and disclosure of PHI
3. Minimum Necessary and Oral Communications
 - Incidental disclosures of PHI, such as occur when someone overhears a fragment of a conversation between doctors and other professionals, would not be considered an impermissible disclosure (and thus, subject to fines and penalties)
4. Business Associates
 - The proposal includes model business associate contracts
 - An extension of an additional year would be allowed to change existing contracts
5. Marketing
 - Covered entities would be explicitly required to obtain an individuals' specific authorization before sending them any marketing materials
6. Parents and Minors
 - State law will govern disclosures to parents
 - If state law is silent or unclear, a health care provider may use discretion to provide or deny a parent access to records as long as that decision is consistent with the state or other law
7. Uses and Disclosures for Research Purposes
 - Researchers would no longer be required to use multiple consent forms (e.g., one for informed consent to the research and one related to their privacy rights).

MORE HIPAA

HIPAA covers many other aspects of our practice. Future articles will detail these issues. Remember, APA will take the lead in providing you with the necessary resources and information to ensure that you will be able to comply with HIPAA. MPA will continue to provide additional information, offer workshops, and be an ongoing personal resource for you and for all MPA members.

