getting ready for

HIPAA

what you need to know *now*

a primer for psychologists

inside:

The facts about HIPAA

How psychologists will be affected

The consequences of failing to comply

Where to turn for resources and help

march 2002

AMERICAN PSYCHOLOGICAL ASSOCIATION PRACTICE ORGANIZATION

THE TRUST

COUNTDOWN TO 2003:
HELPING PSYCHOLOGISTS COMPLY

April 14, 2003: The initial deadline for compliance with the privacy rule of the Health Insurance Portability and Accountability Act (HIPAA). The coming year will provide the necessary lead time to raise awareness among practitioners, identify important issues and complete the steps that will lead to HIPAA compliance. As part of the process, the APA Practice Organization has been engaged in ongoing dialogue with practitioners and with the Department of Health and Human Services (HHS) to help apply the privacy rule to the practice of psychology.

This primer has been prepared by the APA Practice Organization (the Practice Organization) and the APA Insurance Trust (the Trust). It is intended primarily for psychologists in private practice. The primer will also be useful to psychologists who work in other settings such as hospitals, integrated delivery systems, clinics, university health and counseling centers and schools as they participate in the HIPAA compliance processes and procedures that those organizations are required to create and implement.

Consultation on HIPAA issues will be available from the APA Practice Organization and, for those insured in the Trust-sponsored Professional Liability Insurance Program, from the Trust 800 Risk Management Program.

TABLE OF CONTENTS

WHAT IS HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) was the result of a bill sponsored by Senators Nancy Kassebaum (R-KS) and Ted Kennedy (D-MA), which was signed into law in August 1996.

The act was designed to protect Americans who were previously ill from losing their health insurance when they changed jobs or residences. Another major intent of the law was to streamline the health care system through the adoption of consistent standards for transmitting uniform electronic health care claims. In order to make this work, it also became necessary to adopt standards for securing the storage of that information and for protecting an individual's privacy. When the rules are in place, it is believed that the health care industry will have a standardized way of transmitting electronic claims with increased privacy and security protection for the electronic dissemination of health care information.

PRIVACY AND CONFIDENTIALITY

The privacy rule came to be part of the HIPAA statute as the result of a self-imposed deadline created by Congress. If Congress failed to enact comprehensive health information privacy legislation by August 21, 1999, the statute required the Secretary of HHS to promulgate privacy regulations. As we now know, Congress failed to act, and HHS promulgated a final privacy rule that became effective on April 14, 2001, with an expected compliance date of April 14, 2003.

The two-year delayed implementation period was intended to provide substantial time for professional associations, such as APA, to work with their members to assess the effects of the privacy rule and to develop necessary policies, protocols and procedures to comply with it. Additionally, HHS expects to work with APA and other trade and professional associations to develop guidance and provide technical assistance so that they can help their members understand and comply with the privacy rule.

TRANSACTION AND SECURITY RULES

In addition to the privacy rule, two other rules must be mentioned:

The first, often referred to as the "transaction rule," requires standard formatting of electronic transactions for certain specified financial and administrative purposes such as health care claims or inquiries about plan eligibility or plan coverage. Initially, the rule was released in October 1999, with a compliance date of October 2002. This date has now been moved to October 2003. However, HHS will be developing a form that they will require psychologists to submit by October 16, 2002, describing how they plan to meet the "transaction rule" requirements by the official deadline. It should also be noted that:

- There is no provider obligation to engage in electronic claims submission (i.e., it is voluntary).
- For those who choose to transmit claims electronically, practice management software or an outside party such as a health care clearinghouse will be needed to handle the conversion of data to meet the requirements.

The second is a rule focusing on security, which has not yet been released in final form.

DIFFERENCES BETWEEN THE PRIVACY AND SECURITY RULES

Although the security rule is not completed, it is helpful to clarify the differences between the privacy and security rules.

- The privacy rule focuses on the application of effective policies, procedures and business service agreements to control the access and use of patient information.
- The proposed security rule addresses the provider/organization's physical infrastructure such as access to offices, files and computers to assure secure and private communication and maintenance of confidential patient information.

GOVERNMENT ENFORCEMENT AND PENALTIES

Formal compliance with the HIPAA requirements is a necessity because there are real and significant penalties for non-compliance. If a health care provider refuses to become informed or deliberately fails to take appropriate action, the consequences of failing to comply with HIPAA include (from the least to the most severe):

- Administrative action taken by the HHS Office for Civil Rights.
- Civil Penalties of not more than $100 for each violation with the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year not to exceed $25,000.
- Fines of up to $250,000, imprisonment for up to 10 years, or both for knowingly violating "wrongful disclosure of individually identifiable health information."

It should also be mentioned that a primary initial aim of the HHS Office for Civil Rights is to work with the health care community to help them understand and implement HIPAA.

HOW WILL HIPAA'S PRIVACY RULE AFFECT YOUR PRACTICE?

Even though psychologists have always placed a high priority on safeguarding patient confidentiality, the privacy rule will increase privacy protection for all health information.

In general, the privacy rule will require psychologists to:

- Provide information to patients about their privacy rights and how that information can be used.
- Adopt clear privacy procedures for their practices.
- Train employees so that they understand the privacy procedures.
- Designate an individual to be responsible for seeing that privacy procedures are adopted and followed.
- Secure patient records.

The privacy rule was developed with the understanding that there are many different types of health care providers who must comply, ranging from large multi-hospital systems to individual solo practitioners. Therefore, the administrative and procedural requirements are designed around the notion of "scalable compliance."

SCALABLE COMPLIANCE

The administrative requirements of the privacy rule are "scalable," meaning that a covered entity takes "reasonable" steps to meet the requirements according to its size and type of activities. In other words, the administrative burden on a psychologist who is a solo practitioner will be far less than that imposed on a hospital. For example, a hospital may be required to create a full-time staff position to serve as a privacy officer, while a psychologist may identify him- or herself as the "privacy officer" in a solo practice.

ABOUT THE PRIVACY RULE

The HIPAA privacy rule was designed to serve as a minimum level of privacy protection. Thus, it only takes precedence over state laws that provide less privacy protection or that provide patients with less access to and control over their health information. State laws that provide better protection from the consumer's vantage point are not pre-empted by HIPAA. In those situations, psychologists should follow state law. This approach provides better protection for patients, but it also means that HIPAA expects health care providers to be aware of all state laws where they practice that pertain to the privacy of health care information.

The Practice Organization and the Trust, in collaboration with the state psychological associations, have already begun an analysis that will provide practitioners with guidance on compliance issues regarding the interaction of state laws and HIPAA before the effective date of the regulations. Pre-emption of state laws is discussed in detail later in this document.

TO WHOM DOES THE PRIVACY RULE APPLY?

The HIPAA privacy rule applies to "covered entities" including:

- Health care providers
- Health plans (including employer-sponsored group plans, Medicaid, Medicare, etc.)
- Health care clearinghouses

In a different and indirect way, the privacy rule also applies to those doing business with covered entities (i.e., business associates) through contract terms with such entities. Business associates are discussed in detail later in this document.

TO WHAT KIND OF INFORMATION DOES THE PRIVACY RULE APPLY?

In order to understand how the privacy rule treats health information, it is important to briefly review four definitions that are included in the rule: "Health Information," "Individually Identifiable Health Information," "Protected Health Information," and "Psychotherapy Notes." The definitions for these terms are very specific but are summarized as follows:

- **Health Information:** Any information, whether oral or recorded in any form, created or used by health care professionals or health care entities.
- **Individually Identifiable Health Information:** A subset of Health Information that either identifies the individual or that can be used to identify the individual.
- **Protected Health Information (PHI):** Individually Identifiable Health Information becomes Protected Health Information (PHI) when it is transmitted or maintained in any form or medium. More specifically, PHI is information that relates to the past, present or future physical or mental health condition of an individual; the 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.
- **Psychotherapy Notes:** Notes recorded in any medium by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint or family counseling session, and that are separated from the rest of the individual's medical record.

  The definition in the privacy rule specifically *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, the treatment plan, symptoms, prognosis and progress to date.

The privacy rule applies to Protected Health Information (PHI). Health information that does not identify an individual and provides no reasonable basis to believe that the information can be used to identify a person is not considered PHI. PHI also excludes Individually Identifiable Health Information in educational records covered by the Family and Educational Right and Privacy Act. (20 U.S.C. 1232g).

WHAT ARE THE TRIGGERS?

Application of the privacy rule is triggered when:

- A psychologist transmits PHI in electronic form in connection with any of the following types of transactions:
  - Health care claims
  - Health care payment and remittance advice
  - Coordination of benefits
  - Health care claim status, enrollment or dis-enrollment in a health plan
  - Eligibility for a health plan
  - Health plan premium payments
  - Referral certification and authorization
  - First report of injury
  - Health claims attachments

- An entity acting on behalf of the psychologist transmits health information in electronic form, such as a billing service. This means that psychologists who directly or indirectly accept third-party reimbursement for health services must comply with HIPAA.

Once triggered, the privacy rule applies to a psychologist's entire operation, not just to information in electronic form. The privacy rule does not allow for a psychologist to segregate that part of his or her practice to which HIPAA standards apply.

Although it is theoretically possible for a psychologist who has an entirely self-pay practice and who does not use electronic record keeping to not trigger the privacy rule, it is recommended that all psychologists make their practices HIPAA compliant by the April 2003 deadline. By doing so, they will ensure that any future actions they may take do not place them in violation of HIPAA compliance regulations. For example, should he or she decide at some point to accept third-party reimbursement, to employ electronic record keeping, or to employ a billing service, he or she will have to be in compliance immediately upon doing so and will not be given any grace period for meeting HIPAA requirements.

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), leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk or compact-disk media.

FAXES

The following examples illustrate why it is recommended that all faxes be treated as if HIPAA applies:

- If the original fax is generated on a computer or sent via the computer rather than a fax machine, then an electronic copy of the document exists even if the document has been erased (i.e., a recoverable copy usually stays on the computer drive even after it has been deleted).
- When a psychologist receives a fax, he or she has no way of knowing whether it has been created, stored or sent electronically (e.g., from a computer equipped with fax software and a modem) and is therefore considered to be PHI.

In order to be in compliance with HIPAA, psychologists will need to have a policy that states how the confidentiality of faxes will be handled; procedures for attaining confidentiality; and a documented process for implementing the policy and procedures (e.g., training, monitoring, auditing, etc.).

GENERAL PROVISIONS UNDER THE PRIVACY RULE

It is important to understand the general provisions relating to consent, authorization for the release of psychotherapy notes and minimum necessary disclosure.

CONSENT

Psychologists must obtain a patient's consent prior to using PHI to carry out "treatment," "payment," and "health care operations." A generalized consent form will be necessary when dealing with third parties and, as a practical matter, should be secured at the outset of treatment rather than waiting until the information is shared. This form differs from and is not a substitute for the "informed consent"* that is also typically obtained prior to the initiation of treatment.

Providers can secure both forms of consent at the same time; however, the generalized consent form must be visually and organizationally separate from other legal permission and must be separately signed and dated. The consent form must indicate that the individual has the right to revoke consent in writing. Any actions the psychologist may have taken before receiving notice that the consent has been revoked would not be covered by the revocation.

*An example of a model informed consent contract can be downloaded from the Trust Web site at APAIT.org. A model HIPAA general consent form is being developed and will be included in future resources for psychologists.

DEFINITIONS

Health Care: Care, services or supplies related to the health of an individual including but not limited to the following: preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and the sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Treatment: The provision, coordination or management of health care and related services by one or more health providers. The treatment definition includes consultation between health care providers relating to a patient or the referral of a patient from one health care provider to another.

Payment: For psychologists, payment refers to the activities one undertakes to obtain reimbursement for health care services that have been provided. These activities can include, among others: determinations for eligibility or coverage, billing, claims management, collection activities and utilization review.

Health Care Operations: Health care operations is a very broad category of activities ranging from quality assessment and utilization review to conducting or arranging for medical reviews, legal services and auditing functions, business planning and administrative services.

The consent is valid for:

- Use by the originator of the psychotherapy notes for treatment (disclosure of the psychotherapy notes requires specific authorization, which is discussed in the next section of this document).
- Use or disclosure by the covered entity in training programs in which students, trainees or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family or individual counseling.
- Use or disclosure by the covered entity to defend a legal action or other proceeding brought by an individual.

Patient consent is not required for the following:

- If the psychologist has an indirect relationship with the patient. For example, when a health care provider delivers health care based on the orders of another health care provider; or when a provider delivers services, products or reports and the results go to another provider who works with the patient (e.g., if a psychologist performed psychological testing and the results were sent to the patient's physician or psychotherapist).
- In an emergency situation (consent will need to be obtained as soon as possible afterward).
- If the psychologist has to treat the patient by law and he or she has attempted but was not able to get consent.
- If the psychologist is unable to get consent due to "substantial" barriers in communication, and consent is conferred.
- For health oversight activities authorized by law.

Any use of PHI for purposes other than treatment, payment or health care operations also **requires patient authorization** (See next section on "Patient Authorization"); that is, specific written permission above and beyond the general consent already obtained. For example, if a psychologist receives a request for information from an employer or school that is not part of the billing procedures or claims process, he or she cannot release it without patient authorization.

Psychologists will have to document attempts to get consent and keep signed consents in accordance with the privacy rule's documentation requirements.

PATIENT AUTHORIZATION FOR RELEASE OF PSYCHOTHERAPY NOTES

During the rule-making process, the APA Practice Organization successfully communicated to HHS the recommendation that a specific authorization process for psychotherapy notes be included in the requirements. The final privacy rule contained a definition of psychotherapy notes similar to what we in the profession have historically referred to as "process notes."

Authorizations are forms that psychologists typically refer to as releases, which meet certain requirements specified by the privacy rule. Briefly stated, an authorization must contain 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 disclosure
- An expiration date
- The right to revoke
- The right not to authorize the disclosure

The privacy rule states that general consent alone is insufficient when a third party requests psychotherapy notes; it requires psychologists (and other "covered entities") to obtain specific patient authorization for the use and disclosure of such notes.

Psychologists will have to ensure that any entity requesting psychotherapy notes has provided a valid authorization before releasing those notes. Or, alternatively, psychologists will have to secure authorization from the patient before providing information contained within the psychotherapy notes in response to requests. Additionally, when seeking consultation from another provider for treatment purposes, patient authorization must be obtained in order to disclose information in psychotherapy notes that has not been de-identified.

In the regulatory definition, one of the requirements for notes to qualify as "psychotherapy notes" is that they must be "separated from the rest of an individual's medical record." Currently, it is not clear whether this will require psychologists to keep two physically separate records – one for psychotherapy notes and one for all other health information – or whether such information can be excerpted from psychologists' psychotherapy notes upon appropriate request. Due to the additional protection associated with psychotherapy notes, a conservative analysis is that psychologists will have to segregate this information for purposes of transactions and ensure that increased procedural requirements for psychotherapy notes are met.

WHEN NO CONSENT OR AUTHORIZATION IS REQUIRED

Neither consent nor authorization is required for use and disclosure of PHI, including psychotherapy notes, in the following instances:

- To show compliance with the privacy rule
- When required by law
- For health oversight activities of the originator of the psychotherapy notes
- To a coroner or medical examiner for identification, cause of death, or other duties authorized by law (will be subject to state pre-emption)
- To avert a serious threat to the health or safety of a person or the public (explained in detail later in this document)

MANAGED CARE AND INSURANCE COMPANIES

A covered entity, such as a managed care or insurance company, or an ERISA-certified employee benefit plan, is prohibited from conditioning treatment, eligibility for benefits or payment of claims on the patient's authorization to disclose psychotherapy notes. This eliminates one of the biggest complaints from practitioners and consumers about intrusive requests for information from managed care companies.

MINIMUM NECESSARY DISCLOSURE

When PHI is disclosed or used, the privacy rule requires psychologists to share the minimum amount of information necessary to conduct the activity. A couple of important points to note:

- The privacy rule also applies to PHI available internally to employees so they can do their jobs (e.g., a billing clerk may have access to the minimum amount of information needed to perform the billing role that would not include clinical information).
- In a treatment context, the minimum necessary provision does not apply. Therefore, psychologists are free, as permitted by state law, to share information they wish with another provider for the purpose of providing treatment, as permitted by authorization.
- Minimum necessary disclosure does not apply to requests for information that require authorization above and beyond the general consent, such as with psychotherapy notes. This is because the information to be disclosed is specifically described by the authorization itself.

FOCUS: *USE AND DISCLOSURE*

There are a number of circumstances in which the privacy rule permits psychologists to make certain disclosures without consent or authorization. These may include providing information to:

- A public health authority
- A health oversight agency
- A coroner or medical examiner
- The military, Veterans Affairs or another entity for national security purposes
- A hospital or other type of facility for its facility directory

In addition, psychologists may disclose PHI without consent and authorization for purposes related to:

- Workers' Compensation Laws
- Victims of abuse, neglect and domestic violence
- Other situations as required by law

Specific provisions for use and disclosure of PHI in all of the situations mentioned above have been identified within the privacy rule and will be elaborated on in greater detail in subsequent materials and resources.

DEFINITION

Use and Disclosure: The privacy rule defines a "use" as the sharing, employment, application, utilization, examination or analysis of individually identifiable health information within an entity that maintains such information.

The privacy rule defines a "disclosure" as the release, transfer, provision or access to, or divulging in any other manner of information outside the entity holding the information.

FOCUS: PRE-EMPTION OF STATE LAWS

The privacy rule establishes a minimum set of requirements for the protection of PHI. As a result, state laws are not pre-empted to the extent that they are stricter in protecting an individual's PHI.

State laws that are either contrary to or not as strict as HIPAA in protecting an individual's PHI will be pre-empted by HIPAA and therefore give way to the federal rule.

CONTRARY STATE LAWS

"Contrary" means that a psychologist would find it impossible to comply with both the state and federal requirements, or that the state law stands as an obstacle to the purposes and objects of the HIPAA privacy rule. In other words, a state law offering less privacy protection would be superceded by the privacy rule (see "Pre-emption Analysis Steps" in the next section). There are, however, four exceptions regarding pre-emption of state law by the privacy rule:

- When state law provides for the reporting of disease or injury, child abuse, births or deaths, or for the conduct of public health surveillance, investigation or intervention
- 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
- When state law relates to the privacy of health information and is more stringent than the HIPAA privacy rule
- When, at the request of a state governor, the Secretary of HHS determines 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
  - For purposes of serving a compelling need related to public health, safety or welfare.

It should be noted that the latter is a formal process to be conducted by the state. It is not intended for psychologists and other health care providers to exercise independent judgment in these situations.

PRE-EMPTION ANALYSIS STEPS

HIPAA assumes that psychologists are familiar with existing state laws related to the privacy protection of health care information. Under HIPAA, it will be necessary to determine if a state law is stricter or more stringent in its protection of health information. This is what is referred to as a "pre-emption analysis." The first step in this analysis is to determine if the state law relates to the privacy of health information.

- The law "relates" if it has "the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear and substantial way."
- The law need not be labeled a privacy law.

The second step is to determine whether the state law is more stringent than the privacy rule. In this context, "more stringent" is viewed from the consumer's perspective. Answers to the following questions will help to make that determination:

- Is more information protected or are there greater requirements for authorization or consent to disclose under the state law or under HIPAA?
- Under which law is more access afforded to the individual to view one's own records or does a greater right exist to amend one's own records?
- Which law requires higher record-keeping standards that allow individuals to monitor disclosures?

It should also be noted that:

- The definition of "more stringent" explicitly includes a provision that preserves state laws governing the rights of minors to obtain health care without parental knowledge (i.e., such laws are not pre-empted by HIPAA).

- HHS will not make determinations as to whether a state law is or is not more stringent. For example, if a psychologist chooses to ignore a state privacy law thought to be less stringent and exclusively follows the federal rule, only a state enforcement action against the psychologist and subsequent judicial decision will settle the issue.
- The privacy rule pre-empts on a provision-by-provision basis, not law-by-law. In other words, if one provision of a state privacy law is pre-empted, another may not be.
- Even if a state privacy law is "saved" from pre-emption (i.e., not pre-empted by HIPAA), it would still not apply if otherwise pre-empted by ERISA.

When there is doubt about whether to apply the federal rule or state law, guidance will be needed from HHS and the states. The APA Practice Organization, the Trust and State Psychological Associations are taking a leading role in analyzing and addressing state pre-emption issues.

FOCUS: *DEALING WITH THE JUDICIAL SYSTEM AND ADMINISTRATIVE PROCEEDINGS*

Requests for information for judicial and administrative proceedings is one area where mental health records will receive greater protection than other health records as a result of more stringent state laws.

According to the general rule, PHI can be disclosed without consent, authorization or an opportunity for the patient to object:

- In response to a court order (including subpoenas that are court-ordered)
- On order from an administrative tribunal (e.g., the Social Security Administration)

The HIPAA privacy rule also directs instances in which PHI may be disclosed without a court order and without consent, authorization or an opportunity for the patient to object. According to the privacy rule, PHI may also be disclosed in response to a non-court-ordered subpoena, discovery request or other legal process not accompanied by a court order if "satisfactory assurance" is provided. "Satisfactory assurance" must demonstrate that reasonable efforts have been made to ensure that the patient has been given notice of the request or that reasonable efforts have been made to secure a qualified protective order.

However, virtually all states' psychotherapist-patient privilege communications statutes are more stringent than this HIPAA provision. Information acquired in the course of the psychotherapy relationship cannot be disclosed without specific authorization by the patient or a court order. Such state laws would take precedence over HIPAA.

FOCUS: *DEALING WITH LAW ENFORCEMENT AGENCIES*

A psychologist may disclose PHI for a law enforcement purpose to a law enforcement official under certain circumstances:

- As required by law, or
- In compliance with any of the following:
  - A court order or court-ordered warrant, subpoena or summons issued by a judicial officer
  - A grand jury subpoena
  - An administrative request, including an administrative subpoena or summons, civil or authorized investigative demand or similar process authorized by law. In the latter situation, the following conditions must be met: the information being sought must be relevant to a legitimate law enforcement inquiry; the request must be specific and limited in scope to the purpose for which it is requested; and any de-identified information cannot reasonably be used.

There are a number of other provisions pertaining to law enforcement agencies and their pursuit of suspects, fugitives from justice and desired witnesses. Many of these provisions are intended to deal with a scenario in which the individual

being sought may be injured and is seeking medical treatment. While not impossible, psychologists are not likely to encounter this type of occurrence. Nonetheless, because this represents a very new approach for federal law, the Practice Organization and the Trust will continue to analyze these provisions to determine how they may affect psychologists and how they will interact with relevant state law.

DISCLOSURE TO AVERT A SERIOUS THREAT TO HEALTH OR SAFETY

Consistent with applicable law and professional ethics, a psychologist may disclose PHI without consent or authorization to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. The disclosure can only be made to a person or persons reasonably able to prevent or lessen the threat – including the target of the threat. This permitted disclosure is generally consistent with the disclosures covered by Tarasoff-type duty to protect laws.

HHS intends this disclosure to be very narrow and to apply only in "rare circumstances," thus not creating any "duty to warn" other than that which already exists in law. However, the privacy rule is broad in its application to all covered entities, from psychologists and other therapists to health care professionals. Therefore, any covered entity may disclose with a presumed "good-faith belief" to avert a serious threat to health or safety.

The privacy rule also appears to allow psychologists to disclose information in which there is a serious and imminent risk that their patient may attempt suicide. For example, this information may be communicated to the police, to a hospital, or to family members who could be expected to protect the individual.

It is also worth noting that the privacy rule permits disclosure in situations in which individuals admit to participating in a violent crime, although such statements made in the course of psychotherapy are typically prohibited from disclosure by state law. Given this exemption, it appears that this provision would apply to psychologists only in the rarest of circumstances.

FOCUS: *PATIENTS – THEIR RIGHTS AND RECORDS*

Under HIPAA, patients in many states will now have greater access to their records and greater knowledge of how their records will be used than ever before. They will also benefit from the enhanced protection of psychotherapy notes.

Patients have the right to:

- Receive notice of use and disclosure of their PHI
- Consent to use and disclosure of their PHI
- Access their records for inspection and amendment
- An accounting of how their PHI was used and shared

NOTICE

Under the HIPAA privacy rule, patients have the right of notice. This means the obligation is on the psychologist to inform patients about potential uses and disclosures of their PHI and their right to limit those uses and disclosures. Provision of health care services may be conditioned on the patient's willingness to provide consent to disclose.

PATIENT REQUESTS FOR RESTRICTIONS

As part of the consent process, psychologists must inform individuals that they have the right to request restrictions on the use and disclosures of PHI for treatment, payment and health care operations purposes. The consent also must state that the psychologist is not required to agree to an individual's request. However, the psychologist must agree to "reasonable requests" for restrictions such as a request that information not be sent to specific individuals or a request that information be sent to a particular location. If the psychologist does agree to a particular restriction, that agreement is binding.

As is currently the case, psychologists are not required to accept disclosure restrictions that could compromise their professional judgment or conclusions.

PATIENT ACCESS TO RECORDS

With limited exception, a patient is allowed to inspect and obtain a copy of PHI in a designated record set. The privacy rule defines a "designated record set" as the medical and billing records maintained by the provider and used to make decisions about the patient. Psychologists can require that the request be made in writing. In most cases, the request must be fulfilled within 30 days.

Patients *do not* have the right to:

- Inspect or obtain a copy of psychotherapy notes
- Inspect information compiled in "reasonable anticipation" of, or for use in, a civil, criminal or administrative action
- Access information systems that are used for quality control or peer-review analysis

Psychologists will be required to have policies and procedures for assuring individuals' access to their PHI. This will include putting a process in place to document the records that are accessed and by whom.

It is important to note that in states that have laws guaranteeing patient access to all the psychologist's records, including psychotherapy notes, these laws will apply since they enhance a patient's right of access to information.

PATIENT AMENDMENT OF RECORDS

"Right of amendment" refers to patients' ability to request a change in their PHI if they feel the PHI is incorrect. A psychologist can deny requests for record amendments if he or she is not the originator of the information or if the information is accurate and complete.

Exception: If an individual provides a reasonable basis to believe that the originator of PHI is no longer available to act on the request, the psychologist must address the request as though he or she created the information. There will be a formal process for granting and denying requests to amend records.

Providers will be required to develop a procedure for granting and denying requests to amend records, which are governed by a relatively complex set of rules.* All communication relating to granting and denying requests must be included in a patient's record.

Any changes resulting from an amendment to the record **do not expunge any prior information or part of the record;** it is simply added to it.

ACCOUNTING FOR DISCLOSURES

"Right of accounting" refers to the individual's right to receive a listing of all disclosures of any PHI for the previous six years in which the information has been maintained.

Tracking must begin on the scheduled compliance date. It will not be required for occurrences before that date. The accounting for each disclosure must include the date, name and address of the entity receiving the PHI, a brief description of what was disclosed and a brief statement of the purpose of the disclosure or, in place of such a statement, a copy of the patient's written authorization.

An accounting must be made within 60 days of the request. Individuals have the right to receive one free accounting per twelve-month period. For each additional accounting, a psychologist may charge a reasonable cost-based fee.

Individuals do not have the right to accounting for disclosures:

- To health oversight or law enforcement agencies under special circumstances when such a disclosure might impede the agency's activities
- Used for a facility directory
- To persons involved in the individual's care
- For national security and intelligence purposes
- To correctional institutions or law enforcement officials

*The APA Practice Organization and the Trust are developing the full set of resources needed to help psychologists understand HIPAA in the context of their own practices and take appropriate action. These resources will include model forms, policies and procedures such as the ones necessary for granting and denying requests to amend records.

- Made by the psychologist prior to the compliance date
- About their own access to their records
- To HHS regarding compliance under the privacy rule
- To business associates and personal and legal representatives under special circumstances

RETALIATORY ACTION

A psychologist may not intimidate, threaten, coerce, discriminate or take other retaliatory action against a patient for:

- Exercising a right or participating in any other allowable process under the privacy rule
- Filing an HHS compliance complaint
- Testifying, assisting or participating in a compliance review, proceeding or hearing
- Opposing any act or practice in which the patient or the patient's representative has a "good-faith belief" that the practice is unlawful and where the manner of opposition is reasonable and does not involve disclosure of PHI

WAIVER OF RIGHTS

Patients cannot be required to waive their right to file an HHS compliance complaint as a condition of the provision of treatment.

FOCUS: PERSONAL AND LEGAL REPRESENTATIVES

A psychologist must treat a personal or legal representative of the patient as if he or she were the patient. Personal representatives include those for adults and emancipated minors.

A psychologist may refuse to treat an individual as a personal representative of the patient under the following conditions:

- If there is reason to believe that the patient has been or may have been subjected to domestic violence, abuse or neglect; or there is reason to believe that treating the person as a personal representative could endanger the individual; and
- If he or she decides "in the exercise of professional judgment" that treating an individual as a personal representative is not in the best interest of the patient

These consent and disclosure requirements also apply to the legal representatives of deceased individuals. There are, however, many state statutes that preserve psychotherapeutic confidentiality and privilege even after the death of a patient and would thus take precedence over the privacy rule.

FOCUS: MINORS

The privacy rule indicates that because parents generally have the authority to make health care decisions about their minor children, they (parents) are generally recognized as personal representatives and can therefore access PHI about their children. There are three exceptions to this provision:

- If a state law allows a minor to access mental health services without the consent of a parent
- When a court makes the determination or a law authorizes someone other than the parent to make health care decisions for the minor
- When the parent/guardian/person legally acting as the parent assents to an agreement of confidentiality between the minor and the health care professional

Under these exceptions, the privacy rule makes clear that although records do not have to be disclosed, the minor may still voluntarily choose to involve a parent or other adult. However, if the minor does choose to involve a parent or adult, the minor maintains the exclusive ability to exercise his or her rights under the privacy rule to preserve the confidentiality of PHI. The privacy rule also clarifies that when a parent, guardian or other legal representative for a child or minor signs an authorization for the release of records, it remains valid even when the child becomes an adult until it is revoked or expires.

DEFINITION

Business Associate: A "business associate" is an organization or person other than a member of the psychologist's workforce who receives PHI from the psychologist to provide services to, or on behalf of, the psychologist (e.g., accountant, lawyer, billing service, collection agency). A business associate is not considered a covered entity by HIPAA.

FOCUS: BUSINESS ASSOCIATES

PHI may be disclosed to a business associate. However, psychologists will need to obtain "satisfactory assurance" in the form of a written contract that the business associate will appropriately safeguard the information.

A business associate contract must clearly establish what is permitted and required regarding use and disclosure of records. Subcontractors must also agree to all of the contract's conditions and restrictions. In effect, the psychologist will need to contractually obligate the business associate to follow all the HIPAA compliance requirements the psychologist is required to follow.

Once a business associate contract is in place, the respective parties must monitor the agreement to ensure that all terms of the contract are met. If a psychologist knows that a business associate is breaching or violating his or her obligation under their contract, he or she will have to take reasonable steps to cure the breach. If those steps are unsuccessful, the psychologist may have to terminate the contract and/or report the problem to HHS.

A business associate relationship is not created when the psychologist:

- Furnishes PHI to a postal or courier service
- Discloses PHI to federal oversight health agencies such as the Medicare Peer Review Organization (PRO)
- Responds to a law enforcement request
- Discloses within a covered entity (e.g., the psychologist's own group practice)
- Discloses for purposes related to treatment (For example, a disclosure by a psychologist to a health care provider covering treatment of an individual does not create a business associate relationship.)

Exception: Persons participating in health care treatment generally are not considered to be business associates. However, another health care provider such as a hospital performing non-health-care services for psychologists such as billing is considered a business associate.

MISCELLANEOUS

MARKETING AND FUND RAISING

"Marketing" is defined by the privacy rule to mean the making of a communication about a product or service for the purpose of encouraging recipients to purchase or use that product or service. Generally speaking, the use of PHI for marketing purposes involves marketing to someone who is or has been a patient, or marketing to an individual because of their diagnosis or condition. For example, hospitals may market to former patients and pharmaceuticals may market to people because of their diagnosis or condition.

In general, patient authorization is required before a covered entity, such as a hospital, is able to use or disclose PHI for marketing purposes. However, the privacy rule has specified some exceptions where PHI may be used or disclosed for marketing purposes without requiring patient authorization:

- No authorization is required when using or disclosing PHI to make a marketing communication to an individual when the communication occurs in a face-to-face encounter with the individual. This means a psychologist may discuss any services or products, including those of a third party, without restriction when meeting with a patient.

- No authorization is required when marketing takes the form of distributing products or services of only nominal value, such as calendars, pens or other merchandise that promotes a health care provider. Patients can also be given free drug samples by an appropriate prescriber if the samples are thought to be useful for their condition.
- No authorization is required when the covered entity is marketing its own health-related products or those of a third party if the communication complies with the following requirements:
  - It identifies the covered entity making the communication.
  - It prominently states that the covered entity is receiving direct or indirect remuneration from a third party for making the communication.
  - It contains instructions describing how the individual may decline to receive future communications about health-related products and services.

Where PHI is used to target the communication about a product or service to individuals based on their health status, it must explain why they have been targeted and how the product or service relates to their health.

The following communications are not considered by the privacy rule to be marketing:

- When it is part of treatment (e.g., making recommendations for specific brand-name pharmaceuticals or making referrals to other health care professionals or facilities).
- When it is made in the course of managing the patient's treatment or recommending alternative treatment (e.g., informing an individual who is a smoker about effective smoking-cessation programs).

DISCLOSING PHI FOR RESEARCH PURPOSES

PHI may be disclosed for research under a limited set of circumstances. Patient authorization is not required if:

- The information has been de-identified (i.e., is no longer PHI)
- There is an approved waiver from an institutional review board
- The information is only being used as preparatory for research (e.g., developing protocols)
- The PHI being used is that of deceased individuals

For additional information regarding disclosing PHI for research purposes, please contact Sangeeta Panicker at 202-336-6000 in the APA Science Directorate.

GRAMM-LEACH-BLILEY ACT

The Gramm-Leach-Bliley Act is referred to by some as "HIPAA Lite." This privacy law dealt with financial information and created compliance requirements for insurers and other financial institutions. States are charged with implementing the Gramm-Leach-Bliley Act. As a result, many mistakenly think that the states are also being charged with HIPAA oversight, which is not the case.

FEDERAL SUBSTANCE ABUSE CONFIDENTIALITY REQUIREMENTS

The federal confidentiality of substance abuse patient records statute establishes confidentiality requirements for patient records that are maintained in connection with the performance of any federally assisted specialized alcohol or drug abuse program. According to an analysis conducted by HHS of the interaction of this law (and regulations) with HIPAA, in most cases a conflict will not exist and health care professionals covered by both will be able to comply with both sets of requirements.

WHAT WILL PSYCHOLOGISTS NEED TO DO?

LEARN ABOUT THE PRIVACY RULE

Psychologists must learn the legal meaning of terms such as "use," "disclosure," "consent" and "authorization" as well as the various types of information that may be kept in health records. A new category of information, "psychotherapy notes," is also part of the regulation and must be understood.

The following is an overview of the types of administrative processes psychologists will be expected to implement in order to meet the requirements of the HIPAA privacy rule:

POLICIES AND PROCEDURES

New office policies and procedures must be implemented with respect to PHI to comply with the requirements of the privacy rule. These policies and procedures must be "promptly" changed, as necessary and appropriate, to comply with any changes in the law that might occur in the future.

ADMINISTRATIVE AND PHYSICAL SAFEGUARDS

Appropriate administrative, technical and physical safeguards must be in place to protect the privacy of PHI. For example, a psychologist should be ready to demonstrate that only he or she has access to the computer in which patient records are kept and that any backup files are accessible only to him or her and that hard copies of such records are locked in a file cabinet. There will likely be some additional requirements when the final security rule is promulgated. The Practice Organization and the Trust will incorporate that information into its HIPAA compliance materials when the information becomes available.

TRAINING

All members of a psychologist's workforce must be trained as necessary and appropriate to carry out their functions under the privacy rule. Training must be documented in accordance with the rule's documentation requirements.

SANCTIONS

A psychologist must have and apply appropriate sanctions against members of his or her workforce who fail to comply with the privacy policies and procedures or requirements of the privacy rule. Sanctions must be documented in accordance with the privacy rule's documentation requirement.

COMPLAINT PROCESS

A patient complaint process regarding compliance with the privacy rule or policies and procedures related to the rule must be in place. This may be as simple as receiving complaints and keeping a file of such complaints.

DOCUMENTATION OF COMPLIANCE PROCEDURES

Policies and procedures must be maintained in either electronic or written form. Various types of HIPAA documentation must be retained for six years from the date of creation or the date when it was last in effect, whichever is later.

DUTY TO MITIGATE

A psychologist must mitigate to the extent practical any harmful effect that he or she knows of regarding his or her employee(s)', or business associate's use or disclosure of PHI in violation of policies and procedures or the requirements of the privacy rule. For example, if the receptionist in a small psychology group practice inadvertently sends the wrong patient records to an insurer for reimbursement, the psychologist might be required to request the records back and inform the patient of the error.

THE APA PRACTICE ORGANIZATION AND THE APA INSURANCE TRUST: YOUR HIPAA RESOURCE

The APA Practice Organization and the Trust are committed to being your HIPAA resource. Our objective is to arm practitioners with the information and tools needed to achieve HIPAA compliance. The information contained in this primer is only the first step.

We are developing a full range of offerings specifically designed to meet the needs of practicing psychologists, including:

- Up-to-date information
- Assessment tools to help you identify your individual practice needs
- The resources needed to take appropriate action such as: model policies and procedures; customizable forms and business associate contracts; and the guidance needed to identify and deal with legal and state pre-emption issues.

You will receive updates on HIPAA in the near future. In the meantime, if you have questions, please contact the APA Practice Organization's Legal and Regulatory Affairs Office at 202-336-5886; or if you have malpractice insurance through the Trust, you can call the Advocate800 Risk Management Consultation Service at 800-477-1200.

THANK YOU.