persons whom the provider believes are reasonably able to prevent or lessen the threat. These provisions may be found in the Privacy Rule at 45 CFR § 164.512(j).

Under these provisions, a health care provider may disclose patient information, including information from mental health records, if necessary, to law enforcement, family members of the patient, or any other persons who may reasonably be able to prevent or lessen the risk of harm. For example, if a mental health professional has a patient who has made a credible threat to inflict serious and imminent bodily harm on one or more persons, HIPAA permits the mental health professional to alert the police, a parent or other family member, school administrators or campus police, and others who may be able to intervene to avert harm from the threat.

In addition to professional ethical standards, most States have laws and/or court decisions which address, and in many instances require, disclosure of patient information to prevent or lessen the risk of harm. Providers should consult the laws applicable to their profession in the States where they practice, as well as 42 USC 290dd-2 and 42 CFR Part 2 under Federal law (governing the disclosure of alcohol and drug abuse treatment records) to understand their duties and authority in situations where they have information indicating a threat to public safety. Note that, where a provider is not subject to such State laws or other ethical standards, the HIPAA permission still would allow disclosures for these purposes to the extent the other conditions of the permission are met.

If a law enforcement officer brings a patient to a hospital or other mental health facility to be placed on a temporary psychiatric hold, and requests to be notified if or when the patient is released, can the facility make that notification?
The Privacy Rule permits a HIPAA covered entity, such as a hospital, to disclose certain protected health information, including the date and time of admission and discharge, in response to a law enforcement official's request, for the purpose of locating or identifying a suspect, fugitive, material witness, or missing person. See 45 CFR § 164.512(f)(2). Under this provision, a covered entity may disclose the following information about an individual: name and address; date and place of birth; social security number; blood type and rh factor; type of injury; date and time of treatment (includes date and time of admission and discharge) or death; and a description of distinguishing physical characteristics (such as height and weight). However, a covered entity may not disclose any protected health information under this provision related to DNA or DNA analysis, dental records, or typing, samples, or analysis of body fluids or tissue. The law enforcement official's request may be made orally or in writing.

Other Privacy Rule provisions also may be relevant depending on the circumstances, such as where a law enforcement official is seeking information

about a person who may not rise to the level of a suspect, fugitive, material witness, or missing person, or needs protected health information not permitted under the above provision. For example, the Privacy Rule's law enforcement provisions also permit a covered entity to respond to an administrative request from a law enforcement official, such as an investigative demand for a patient's protected health information, provided the administrative request includes or is accompanied by a written statement specifying that the information requested is relevant, specific and limited in scope, and that de-identified information would not suffice in that situation. The Rule also permits covered entities to respond to court orders and court-ordered warrants, and subpoenas and summonses issued by judicial officers. See 45 CFR § 164.512(f)(1). Further, to the extent that State law may require providers to make certain disclosures, the Privacy Rule would permit such disclosures of protected health information as "required-by-law" disclosures. See 45 CFR § 164.512(a).

Finally, the Privacy Rule permits a covered health care provider, such as a hospital, to disclose a patient's protected health information, consistent with applicable legal and ethical standards, to avert a serious and imminent threat to the health or safety of the patient or others. Such disclosures may be to law enforcement authorities or any other persons, such as family members, who are able to prevent or lessen the threat. See 45 CFR § 164.512(j).

If a doctor believes that a patient might hurt himself or herself or someone else, is it the duty of the provider to notify the family or law enforcement authorities?

A health care provider's "duty to warn" generally is derived from and defined by standards of ethical conduct and State laws and court decisions such as Tarasoff v. Regents of the University of California. HIPAA permits a covered health care provider to notify a patient's family members of a serious and imminent threat to the health or safety of the patient or others if those family members are in a position to lessen or avert the threat. Thus, to the extent that a provider determines that there is a serious and imminent threat of a patient physically harming self or others, HIPAA would permit the provider to warn the appropriate person(s) of the threat, consistent with his or her professional ethical obligations and State law requirements. See 45 CFR 164.512(j). In addition, even where danger is not imminent, HIPAA permits a covered provider to communicate with a patient's family members, or others involved in the patient's care, to be on watch or ensure compliance with medication regimens, as long as the patient has been provided an opportunity to agree or object to the disclosure and no objection has been made. See 45 CFR 164.510(b)(2).

Does HIPAA prevent a school administrator, or a school doctor or nurse, from sharing concerns about a student's mental health with the student's parents or law enforcement authorities?

Student health information held by a school generally is subject to the Family Educational Rights and Privacy Act (FERPA), not HIPAA. HHS and the Department of Education have developed guidance clarifying the application of HIPAA and FERPA**-**

In the limited circumstances where the HIPAA Privacy Rule, and not FERPA, may apply to health information in the school setting, the Rule allows disclosures to parents of a minor patient or to law enforcement in various situations. For example, parents generally are presumed to be the personal representatives of their unemancipated minor child for HIPAA privacy purposes, such that covered entities may disclose the minor's protected health information to a parent. See 45 CFR § 164.502 (g)(3). In addition, disclosures to prevent or lessen serious and imminent threats to the health or safety of the patient or others are permitted for notification to those who are able to lessen the threat, including law enforcement, parents or others, as relevant. See 45 CFR § 164.512(j).

[1] The Privacy Rule permits, but does not require, providers to disclose information in these situations. Providers who are subject to more stringent privacy standards under other laws, such as certain state confidentiality laws or 42 C.F.R. Part 2, would need to consider whether there is a similar disclosure permission under those laws that would apply in the circumstances.

[2] A parent also may not be a personal representative if there are safety concerns. A provider may decide not to treat the parent as the minor's personal representative if the provider believes that the minor has been or may be subject to violence, abuse, or neglect by the parent or the minor may be endangered by treating the parent as the personal representative; and the provider determines, in the exercise of professional judgment, that it is not in the best interests of the patient to treat the parent as the personal representative. See 45 CFR 164.502(g)(5).

The HIPAA Privacy Rule: Frequently Asked Questions (FAQs)

by Legal and Regulatory Affairs Staff

The Practice Organization has received many questions about what psychologists need to do in light of the April 14, 2003 deadline for complying with the HIPAA Privacy Rule (Privacy Rule). Below are answers to some of the most common questions.

The most complete resource, however, is the HIPAA for Psychologists product that has been developed by the APA Practice Organization and APA Insurance Trust. You can learn more about the product and order it at APApractice.org.

Q: I Send Patient Bills to Insurance Companies Electronically. Does the HIPAA Privacy Rule Apply to Me?

A: Yes, because the Privacy Rule applies to any psychologist who transmits protected health information (see Question 5) in electronic form in connection with a health care claim.

Q: Does the Privacy Rule Apply Only to the Patient Whose Records Are Being Sent Electronically, or Does It Apply to All the Patients in the Practice?

A: Once the rule is triggered (for example by a single electronic transaction as described in the previous answer), the psychologist's entire practice must come into compliance.

Q: Should I Comply with the Privacy Rule If I Do Not Submit Any Claims Electronically?

A: Because the Privacy Rule applies to the electronic transmission of health information, some psychologists who do not submit electronic claims or who don't participate with third-party payment plans may not currently need to comply with the Privacy Rule. However, it is in your best interest to comply now, as any number of future actions may trigger the Privacy Rule (for example, participating in Medicare or another third-party payment plan in the increasingly electronic private market). Compliance may also be triggered by actions outside of your control, such as if you use a billing service that becomes entirely electronic. If one of these events suddenly triggers your Privacy Rule obligations after the April 2003 deadline, you will have no grace period for coming into compliance. Consequently, the APA Practice Organization and the APA Insurance Trust strongly recommend that you act now to get in compliance, so that you will be ready as the health care industry becomes increasingly dependent upon electronic transmissions.

Q: Even Though I Do Bill Electronically, I Have a Solo Practice — Basically, It's Just Me. Do I Still Have to Comply with the Privacy Rule?

A: Yes, the Privacy Rule applies to all health care providers — from those in large multihospital systems to individual solo practitioners. The administrative requirements of the Privacy Rule are "scalable," meaning that a covered entity must take "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 in a solo practice may identify him or herself as the "privacy officer."

Q: What Information About My Patients Must I Keep Protected Under the HIPAA Privacy Rule?

A: The Privacy Rule applies to, and provides specific protections for, protected health information (PHI). With certain exceptions, the Privacy Rule defines PHI as information that: (1) is created or used by health care professionals or entities; (2) is transmitted or maintained in any form or medium; (3) identifies or can be used to identify a particular patient; and (4) relates to one of the following: (a) the past, present, or future physical or mental health condition of a patient; (b) the provision of health care to a patient, or (c) the past, present, or future payment for providing health care to a patient.

Q: What Is the Difference Between "Consent" Under the Privacy Rule and "Informed Consent to Treatment?"

A: “Consent,” as it was used in the Privacy Rule, refers to advance permission, typically given by the patient at the start of treatment, for various disclosures of patient information to third parties. Consent is no longer required by the Privacy Rule after the August 2002 revisions. However, in many states this type of consent will still be required for routine disclosures, such as for treatment and payment purposes (these more protective state laws are not preempted by the Privacy Rule).

“Informed consent to treatment” is not a concept found in the Privacy Rule. It refers to a client’s decision to allow a health care provider to perform a particular treatment or intervention. State laws and ethical codes on informed consent require that the psychologist provide understandable information about the risks and benefits so that a patient can make a knowledgeable, informed decision about treatment.

Q: What Are Psychotherapy Notes Under the Privacy Rule?

A: HIPAA defines psychotherapy notes as 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. To meet the definition, these notes must also be kept separate from the rest of the individual’s medical record. The Privacy Rule specifically excludes from the definition information pertaining to counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, medication prescription and monitoring, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. (Psychotherapy notes are similar to, but generally not the same as, “personal notes” as defined by a few states.)

Q: Is There Any Special Protection for Psychotherapy Notes Under the Privacy Rule?

A: Yes, the Privacy Rule provides a higher level of protection for psychotherapy notes than for other types of patient information. For example, in most situations you cannot release psychotherapy notes without the patient signing a detailed authorization form specifically for the release of psychotherapy notes. By contrast, in most states you could release the patient’s other records for most treatment and payment purposes without consent, or with just the patient’s signature on a simpler general consent form.

Q: Can My Patient’s Insurance Company Have Access to the Psychotherapy Notes Concerning My Patients? Can the Insurance Company Refuse Reimbursement If My Patient Does Not Authorize Their Release?

A: An insurance company cannot obtain psychotherapy notes without the patient's authorization. And the insurance company is not permitted to condition reimbursement on receipt of the patient's authorization for disclosure of psychotherapy notes.

Q: Am I Required to Keep Psychotherapy Notes?

A: No, the Privacy Rule does not require that you keep psychotherapy notes. It simply specifies heightened protection for psychotherapy notes in the event that a psychologist maintains them. Because of that protection, however, it may be advisable to keep psychotherapy notes and use them to protect sensitive information that is not specifically excluded from the psychotherapy notes definition (see Question 8 above).

Q: Do I Have to Get My Patient's Permission Before I Consult with Another Doctor About My Patient?

A: In certain circumstances, the Privacy Rule permits use and disclosure of protected health information without the patient's permission. For example, the Privacy Rule permits consultations between psychologists and other health care professionals without permission, because such consultations fall under the Rule's "treatment" exception. However, many states require that before releasing patient information for a consultation, a psychologist must have obtained the patient's generalized consent at the start of treatment. (Such state laws are not preempted by the Privacy Rule because they are more protective of privacy.) How the Privacy Rule interacts with your state's consent or authorization rules is an important issue covered in the HIPAA for Psychologists product.

Q: I Have Heard the Term "Business Associate" Used in Connection with the Privacy Rule. Who Is Considered a Business Associate, and What Do I Need to Know About Dealing with One?

A: For purposes of the Privacy Rule, business associates include organizations or persons other than a member of the psychologist's office staff who receive protected health information (see Question 5 above) from the psychologist to provide service to, or on behalf of, the psychologist. Examples of "business associates" are billing services, accountants, and attorneys. The Privacy Rule requires that psychologists have a "business associate contract" with any business associates with whom they share PHI. This contract assures that the business associate (who is not directly regulated by the Privacy Rule) will safeguard privacy. HIPAA for Psychologists contains a model business associate contract that you can use in your practice.

Q: Does the Privacy Rule Apply to Industrial/Organizational Psychologists Doing Employment Selection Assessment for Business, Even Though Some I/O Psychologists Do Not Involve Themselves in Psychotherapy or Payment for Health Care?

A: An I/O psychologist simply performing assessment for an employer for an employer's use typically would not need to comply with the Privacy Rule. However, an I/O psychologist or other psychologist performing services for an employer for which insurance reimbursement is sought, or which the employer (acting as a self-insurer) pays for, would have to make sure that the employer is complying with the Privacy Rule.

Q: Does the Privacy Rule Apply to Psychologists in the Military?

A: Military, veterans' affairs and CHAMPUS programs all fall under the definition of "health plan" in the rule. Therefore, the rule applies to the health services provided by these programs. The Secretaries of Veterans' Affairs and Defense are charged with working with the Department of Health and Human Services to apply the Privacy Rule requirements to their respective health programs. Psychologists in these programs should look to their central offices for guidance.

Q: What Is the Security Rule and Has the Final Security Rule Been Released Yet?

A: The Security Rule is one of three rules issued under HIPAA. (The others being the Privacy Rule, which is the primary focus of these FAQs, and the Transaction Rule, which requires standardized formatting of all electronic health care transactions in the health care system. It had an October 2002 compliance date, but psychologists who filed a timely extension form have until October 2003 to comply.) The Security Rule focuses on the physical and technical means of ensuring the privacy of patient information, e.g., locks on file drawers and computer and Internet security systems. The final security rule has not yet been released.

Q: How Can I Find Out More About the Privacy Rule and How to Comply with It?

A: The APA Practice Organization and the APA Insurance Trust have developed comprehensive resources for psychologists that will facilitate compliance with the Privacy Rule. The product, HIPAA for Psychologists, is competitively priced and is now available on the Portal. HIPAA for Psychologists includes:

- Information about how the Privacy Rule applies to psychological practice, how the Privacy Rule preempts and interacts with your state's privacy laws, and what you must do to prepare for the April 14, 2003 compliance deadline;
- The necessary state-specific forms that comply with both the Privacy Rule and relevant state law;
- Policies, procedures and other documents needed to comply with the Privacy Rule in your state;
- Four hours of CE credit from an APA-approved CE Sponsor; and
- A 5 percent premium discount for psychologists insured in the Trust-sponsored Professional Liability Insurance Program for taking the CE course.

In addition to the HIPAA Privacy, Security, and Enforcement Rules, the HIPAA Administrative Simplification Rule also includes the following rules and standards:

Transactions and Codes Set Standards

Transactions are activities involving the transfer of health care information for specific purposes. Under HIPAA, if a health plan or health care provider engages in one of the identified transactions, they must comply with the standard for it, which includes using a standard code set to identify diagnoses and procedures. The Standards for Electronic Transactions and Code Sets, published August 17, 2000 and since modified, adopted standards for several transactions, including claims and encounter information, payment and remittance advice, and claims status. Any health care provider that conducts a standard transaction also must comply with the Privacy Rule.

Identifier Standards for Employers and Providers

HIPAA requires that employers have standard national numbers that identify them on standard transactions. The Employer Identification Number (EIN), issued by the Internal Revenue Service (IRS), was selected as the identifier for employers and was adopted effective July 30, 2002.

HIPAA requires that health care providers have standard national numbers that identify them on standard transactions. The National Provider Identifier (NPI) is a unique identification number for covered health care providers. Covered health care providers and all health plans and health care clearinghouses use the NPIs in the administrative transactions adopted under HIPAA. The NPI is a 10-position, intelligence-free numeric identifier (10-digit number). This means that the numbers do not carry other information about healthcare providers, such as the state in which they live or their medical specialty.

Mindful
Continuing Education

“This course was developed from the public domain document: HIPAA Privacy Rule and Sharing Information Related to Mental Health - U.S. Department of Health and Human Services."