AMERICAN PSYCHOANALYTIC ASSOCIATION

DIRECTIONS FOR COMPLYING WITH HIPAA PRIVACY STANDARDS

Note: These directions were written in 2003 prior to the enactment and implementation of new health information privacy provisions in the HITECH Act, which was enacted on February 17, 2009 as part of the American Reinvestment and Recovery Act. For an analysis of the HITECH Act and particularly the breach notice provisions that became effective on September 23, 2009, go to the following links:

http://www.apsa.org/Portals/1/docs/Members/hippa/HITECH_Act_Overview_APsaA.pdf

http://www.apsa.org/Portals/1/docs/Members/hippa/Breach_Notice_Requirements_APsaA.pdf

I. GENERAL INFORMATION

Beginning on April 14, 2003, all health care providers, including psychoanalysts, **who bill electronically or transmit identifiable health information electronically must be in compliance with the new federal Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule").** The Privacy Rule establishes a federal "floor" of rights that individuals have with respect to the privacy of and access to identifiable health information.

While the Privacy Rule does not include certain rights that individuals have come to expect, practitioners remain subject to **state laws** that provide stronger privacy protections as well as stronger privacy protections in **ethical and professional practice standards and guidelines**, including those adopted by APsaA. In addition, practitioners may afford greater privacy protections than those required by the Rule. The Rule also requires health care providers to furnish a notice to patients of their rights and the providers' responsibilities under federal and state law as well as the privacy practices they adopt. The rights and responsibilities in the notice are to be drawn from the following sources:

A. The federal Privacy Rule;
B. State law, including regulations and case law;
C. The ethics principles and practice standards of the American Psychoanalytic Association and other professional associations; and
D. The practitioners' own privacy policies and procedures.

Failure to comply with the rights and responsibilities set forth in the above sources may result in enforcement actions by federal or state agencies and can result in legal liability in a private lawsuit. Violation of the American Psychoanalytic Association's ethics standards can result in suspension or expulsion from the association. See **American Psychoanalytic Association**, **Principles and Standards of Ethics for Psychoanalysts (rev.'d September 24, 2001)**.

Practitioners who are covered by the new Privacy Rule should have at least the following three documents in place by April 14 or as soon thereafter as possible:

A. a notice of privacy practices (to be furnished to patients on the first service delivery date after April 14, 2003);
B. a written set of privacy policies and procedures; and
C. a "business associates" contract with any entity that handles identifiable health information on behalf of the practitioner.

Purpose of the Privacy Rule

The standards established under the HIPAA Privacy Rule are intended to preserve the public's confidence that the privacy of health information will be protected with the increased use of computers to store and transmit health information. Understanding this intent may be helpful to you in resolving issues that are not specifically addressed in the law.

Who is covered?

The Privacy Rule applies to "covered entities" which include health plans, health care clearinghouses and health care providers who transmit health information electronically. Psychotherapists are included within the definition of health care providers. You will be subject to the rule if you engage in *at least one* standard electronic transaction. A standard transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care, including health care claims, health care payment and remittance advice, coordination of benefits, health care claim status, enrollment and disenrollment in a health plan, eligibility for a health plan, health plan premium payments, referral certification and authorization, first report of injury, and health claims attachments.

Electronic transmission means transmission via the Internet, leased lines, dial-up lines, private networks, and the use of magnetic tape, computer discs or compact disks. A standard electronic transaction includes hiring a billing company to submit your bills electronically or having the hospital where you are admitted to practice submit electronic claims on your behalf.

In addition, even if you do no electronic transmission of data in your private practice, you may be a covered entity if a hospital, clinic or other health care facility where you are employed or work as a consultant bills electronically for your services under your name and provider ID number, even if the facility retains the fees received for your services. This issue is currently being reviewed by the federal Centers for Medicare and Medicaid Service (CMS).

Once you engage in at least one standard electronic transaction after April 14, 2003, all health information you maintain or transmit becomes subject to the Privacy Rule forever, for your entire practice, including paper and oral information.

If you do not transmit health information electronically or bill electronically or you cease engaging in electronic transactions as of the compliance deadline of April 14, 2003, you are not subject to the Privacy Rule and do not have to comply with the

requirements of the Rule. However, if you begin engaging in electronic transactions at any time after April 14, 2003, you will become subject to the Privacy Rule.

Note: According to the latest information from CMS, transmitting health information via a fax machine will constitute an electronic transmission of data *only* if the information is exchanged between **two** computer systems (such as those used by a managed care company). If a provider sends a fax from a paper fax machine, it will not constitute the electronic transmission of data, regardless of who or what type of machine receives the fax.
It is important to remember that most of the provisions of the Privacy Rule apply to all covered entities as well as to psychoanalysts. Therefore, a use or disclosure of identifiable health information by you for one purpose may result in a use or disclosure of that information by the covered entity that receives the information (such as a health plan) for other purposes. In other words, once you disclose patient information, you will no longer be able to limit how it is used.

What is covered?

The Privacy Rule applies to any individually identifiable health information transmitted or maintained in any form. Health information that has been de-identified can be used and disclosed without meeting the privacy requirements of the Rule. In order for information to be considered de-identified, the risk of identifying the individual must be certified as very small or certain identifying characteristics of the information must be removed.

II. PATIENTS' RIGHTS—YOUR RESPONSIBILITIES

Patients' rights

It is important to understand the rights that your patients have under the Privacy Rule in order to understand your responsibilities. Also, a violation of these rights may form the basis for an enforcement or legal action against you. Patients' rights under the Privacy Rule include the following:

1. The right to receive adequate notice of the uses and disclosures of the identifiable health information that you may make and your legal duties with respect to that information.

2. The right to receive a paper copy of that notice, if the notice as been provided electronically.

3. The right to a brief description of how patients may exercise their rights.

4. The right to request restrictions on certain uses and disclosures of identifiable health information including a statement that you are not required to agree to such restrictions.

5. The right to receive confidential communications regarding identifiable health information.

6. The right to inspect and copy identifiable health information, with certain exceptions such as for psychotherapy notes.

7. The right to amend identifiable health information.

8. The right to receive an accounting of disclosures of identifiable health information with certain exceptions, such as disclosures for treatment, payment and health care operations.

Remember that patients may have additional rights under state law and professional standards, and that you may afford additional rights in your privacy policies and procedures.

Your responsibilities

Your responsibilities under the Privacy Rule include the following:

1. To provide the patient with a Notice of Privacy Practices that states that you are required by law to maintain the privacy of identifiable health information and informs the patient of your legal duties and privacy practices with respect to such information.

2. To make a good faith effort to obtain written acknowledgment of receipt of the notice.

3. To have written policies and procedures for the use and disclosure of identifiable health information.

4. To obtain authorization for certain non-routine uses and disclosures. (See section III)

5. To provide an accounting upon request for certain non-routine disclosures.

6. To provide patients with access upon request to identifiable health information with certain exceptions including for psychotherapy notes.

7. To retain written documents required by the Privacy Rule for a period of six years.

As with patients' rights, additional responsibilities may be required by state law and professional standards, and you may assume additional responsibilities in your privacy policies and procedures.

III. USES AND DISCLOSURES UNDER THE PRIVACY RULE

Uses and disclosures without consent

The Privacy Rule states that covered entities may use and disclose identifiable health information for *routine* purposes without consent or any other permission by the patient. Routine purposes are defined as treatment, payment and health care operations. Treatment means the provision, coordination or management of health care and related services undertaken on behalf of a single patient. Payment means activities undertaken to obtain

reimbursement for the provision of health care to an individual. Health care operations, however, means activities that are related to the general business and administrative functions *of the covered entity* regardless of whether they are connected to the treatment or payment of an individual. This may include quality assessment,

accreditation and training, business planning and development, general administrative activities and due diligence in connection with the sale of a covered entity to another covered entity.

The Original Privacy Rule adopted in April of 2001 required patient consent for the use or disclosure of identifiable health information for treatment, payment and health care operations purposes. That requirement was deleted, however, in an amendment to the Rule issued in August of 2002. In addition, HHS stated that the amendment conferred "regulatory permission" on all covered entities to use and disclose identifiable health information for routine purposes without the individual's consent or other permission. Accordingly, the Privacy Rule confers federal regulatory permission on all covered entities, including psychoanalysts, to use and disclose patients' identifiable health information for treatment, payment and health care operations. The Rule permits, but does not require, covered entities to take the patients' wishes and preferences into account. You may experience demands for your patients' mental health information from covered entities who claim to be exercising their new federal right to this information granted by the amended Privacy Rule.

Note that the amended Privacy Rule eliminates the consent requirement *retroactively* in that it permits the use and disclosure of identifiable health information for routine purposes without patient permission regardless of whether the information was created or received before or after the April 14, 2003 compliance date.

While the individual's right of consent is no longer included in the Privacy Rule, the Rule states that you may elect to provide a consent process for your patients at your discretion. Also, consent for the use and disclosure of mental health information is still required under some state laws and ethical standards, including those of the American Psychoanalytic Association. Also, state laws that are more protective of the privacy of health information are not preempted by the Privacy Rule and will continue to apply. Patient consent or permission required by state laws could be written, oral, or implied depending on the specific state law and the circumstances. See Section IV below for a more detailed discussion of how the Privacy Rule interacts with state law.

Ethical and practice standards adopted by the American Psychoanalytic Association state that "The psychoanalyst should never share confidential information about a patient with nonclinical third-parties (e.g., insurance companies) without the patient's, or in the case of a minor patient, the parent's or guardian's informed consent." See **The American Psychoanalytic Association**, **Principles and Standards of Ethics for Psychoanalysts, Guiding General Principle IV. Confidentiality (rev.'d September 24, 2001)**; See also, **American Psychoanalytic Association Practice Bulletin 3, External Review of Psychoanalysis (December 16, 1999)** and **American Psychoanalytic Association Practice Bulletin 2**, **Charting Psychoanalysis, B. Technical Problems in charting psychoanalysis**

(CPT 90845) and derivative psychotherapies, 1. Privacy and Confidentiality (rev.'d October 13, 1995). The APsaA's ethical principles and standards also state that if a third party payer demands that the psychoanalyst act contrary to those principles, "it is ethical for the psychoanalyst to refuse such demands…" **American Psychoanalytic Association**, **Principles and Standards of Ethics for Psychoanalysts, Guiding General Principles, IV. Confidentiality**.
Also, the United States Supreme Court has recognized that communications between patients and their psychotherapists are "privileged" and cannot be disclosed, except in very limited circumstances, unless the privilege is waived by the patient. See Jaffee v. Redmond, 116 S. Ct. 1923 (1996). Recognition of the therapist-patient privilege was based on the Court's finding that the "reason and experience" of the country shows that effective psychotherapy cannot be provided unless the patient can feel confident that communications with a therapist will not be disclosed without permission. While the Court's holding applies to federal law, the Court noted that some form of psychotherapist privilege has been enacted into law by all 50 states and the District of Columbia.

Accordingly, a consent process for the use and disclosure of your patients' mental health information may be required under state law, established ethical standards and federal and state therapist-patient privilege laws. The American Psychoanalytic Association has recently adopted guidelines for informed consent. See **American Psychoanalytic Association, Informed Consent to Review (Approved By Executive Council June 2003).**

It is important to note that the Privacy Rule does not affect existing patients' rights to informed consent for actual medical treatment.

Note also that the Rule permits covered entities to disclose identifiable health information to their "business associates" without patient consent or permission for both routine as well as nonroutine purposes. See section IX for a discussion of business associates.

Uses and disclosures with authorization

The Privacy Rule requires that patients sign an Authorization form for most *non-routine* uses and disclosures of patient health information. A non-routine use or disclosure is a use or disclosure other than for treatment, payment, or health care operations purposes that is not otherwise permitted or required by law. For example, an authorization would be required in connection with a pre-employment medical exam or the release of information to the patient's attorney. An exception to this general rule that is of major importance to psychotherapy is that *authorizations are required for most routine as well as non-routine uses and disclosures of psychotherapy notes.* See section VIII.

The Authorization is a written document that must be prepared on a case-by-case basis and signed by the patient. It must include the name of person or entity to whom the records are being released; a description of the material being released (e.g. medical record for a specified period of time); the purpose or reason for the release (e.g. patient litigation); and the expiration date or expiration event of the Authorization (e.g. December 31, 2003, or "end of litigation"). The Authorization must be maintained in the patient's file, with a copy to the patient.

Note: If the patient is requesting identifiable health information in a situation where an Authorization is required, you may give the information directly to the patient in which case an Authorization would not be required. For example, if your patient requests that you complete a medical form in connection with obtaining a life insurance policy, you may complete the form and give it directly to the patient without an Authorization, even if you know the patient is then going to turn the information over to the life insurance company. Remember, under the Privacy Rule, you are always permitted to provide identifiable health information to the individual who is the subject of that information without consent or authorization. (However, you are not required to grant a patient's request for access to psychotherapy notes, except where otherwise required under state law. See section VIII.) On the other hand, if the patient requests that you mail the medical form directly to the company, an Authorization from the patient is required.

The Privacy Rule provides that having a consent process is *not* a substitute for an authorization required by the Rule. It is possible, therefore, for a use or disclosure to require both consent under state law, professional standards or your own privacy practices *and* authorization under the Privacy Rule. If both are required, the consent may not be combined with the authorization.

Disclosures permitted with an opportunity to agree or object and disclosures required by law/public policy reasons

Covered entities, including psychoanalysts, may disclose identifiable health information without a patient's consent or authorization to a family member, other relative, or close personal friend of the patient if the information is directly relevant to the person's involvement in the patient's care and the patient is informed of the information to be disclosed and is given an opportunity to restrict or prohibit the disclosure. If the patient cannot agree or object because of incapacity or emergency, you may disclose such information if you believe, in the exercise of your professional judgment, that disclosure is in the patient's best interest.

The Privacy Rule also permits covered entities, including psychoanalysts, to make disclosures without patient authorization under certain circumstances when the disclosure is required by another federal or state law or for certain public needs. The purposes for which these unauthorized disclosures can be made include (1) public health activities (e.g., to a public health authority for reporting or controlling disease, injury or disability, to the FDA to track products), (2) prevention of abuse neglect or domestic violence, health oversight (e.g., to a health oversight agency for activities authorized by law), (3) judicial and administrative proceedings (e.g., in response to a court order or subpoena), (4) law enforcement, (5) for identifying deceased individuals, (6) research (if an alteration or waiver of an authorization is obtained from an Institutional Review Board or a privacy board), (7) to avert a serious threat to health or safety (consistent with applicable law and ethical standards), (8) specialized governmental functions (such as military and veterans' activities), and (9) workers' compensation. The above uses and disclosures that are permitted by the Privacy Rule are still subject to provisions of state law that provide more stringent privacy protections or establish specific procedures for such disclosures. They may also be subject to more protective ethical

standards and provisions in your own policies and procedures to the extent that they do not conflict with federal or state law.

APsaA members confronted with a request for disclosure of identifiable health information for one of these purposes may require the requesting entity to set forth the basis in law for the disclosure without patient permission. The Association's ethical standards provide the following guidance:

> "The psychoanalyst should resist disclosing confidential information to the full extent permitted by law. Furthermore, it is ethical, though not required, for a psychoanalyst to refuse legal, civil or administrative demands for such confidential information even in the face of the patient's informed consent and accept instead the legal consequences of such a refusal." **American Psychoanalytic Association, Principles and Standards of Ethics for Psychoanalysts, Guiding General Principle IV. Confidentiality**.

IV. HIPAA PREEMPTION RULE

What is the HIPAA Preemption Rule?

The HIPAA Preemption Rule states that any rule contained in HIPAA that is contrary to a provision of state law will preempt the contrary state law. However, HIPAA privacy and access standards will *not* preempt state law that is more protective of individual privacy or that grants patients greater rights of access to their own health information. (4) state laws relating to the privacy of health information that are more stringent than the privacy requirements under HIPAA. In other words, HIPAA creates a privacy and access floor, which may be augmented by state laws that provide stronger privacy protections or greater access.

Note that state laws that may not be preempted by HIPAA include state constitutions, statutes, regulations, rules, and common law (court decisions that have precedential effect).

How will HIPAA affect the privacy laws in my home state?

According to HHS, about half of the states have statutes that prevent the use or disclosure of at least some identifiable health information without patient permission. The health care licensure laws in most states have general prohibitions on "breaches of confidentiality", and the common law (court made law) in some states recognizes invasion of privacy and breach of a confidential relationship as a cause of legal action under tort law. As stated, the Supreme Court has found that all 50 states and the District of Columbia recognize some form of therapist-patient privilege that is similar to the privilege recognized under federal law.

Providers covered under HIPAA must be familiar with the privacy law in their own state. If your state law provides greater privacy protections or greater rights of access, you should follow your state law with regard to those specific provisions. Furthermore, the documents you use in your practice, including your Policies and Procedures and Notice of Privacy Practices, as described below, must include references to the applicable state laws where appropriate. Several states (such as Maryland and New York) have prepared a preemption analysis that identifies the state health information privacy and access laws that are not

preempted by the Privacy Rule. These analyses are usually available at no, or minimal, charge.

There are currently many versions of the required HIPAA documents in circulation, either from private companies offering a HIPAA packet for sale or from national associations who have prepared HIPAA documents for their members. Although these documents may be accurate with respect to the federal rule, in most cases they will not take into account any of the individual differences or nuances that exist among states. The HIPAA documents and forms you use in your practice must incorporate both the requirements of the federal HIPAA Privacy Rule as well as the requirements of any more restrictive privacy laws in effect in your own jurisdiction. They should also be consistent with the ethical principles and standards of your profession.

V. POLICIES AND PROCEDURES

Providers subject to HIPAA must adopt policies and procedures with respect to protected health information that set forth and implement the standards and requirements of the Privacy Rule, state law, professional standards and the privacy policies you decide to adopt. The policies and procedures must be reasonably designed to ensure compliance with the Privacy Rule and any amendments thereto, taking into account the size and type of activities of your medical office. You must maintain these policies and procedures in written or electronic form, and maintain any communications or documentation required under the policies and procedures for no less than six years.

VI. NOTICE OF PRIVACY PRACTICES\

Health care providers that are covered by the Privacy Rule must prepare and provide to their patients a document called a Notice of Privacy Practices ("Notice"). This Notice must detail the patient's rights and the provider's responsibilities with respect to the use and disclosure of identifiable health information under the Privacy Rule, as well as state law, professional standards and the providers own practices, to the extent that they are more protective of patient rights or grant greater access to information.

How do I distribute the Notice of Privacy Practices to my patients?

You must provide a copy of your Notice to all patients you treat in private practice no later than the date of the first service delivery after April 14, 2003. You are required to make a good faith effort to obtain a written acknowledgement from the patient of receipt of the notice. Retain the acknowledgment form in the patient's medical record. The patient is NOT required to sign the acknowledgment but you must make a reasonable effort to obtain an acknowledgment from each patient you see. If after reasonable efforts, such acknowledgment cannot be obtained, simply make a note of this in the patient's file. In emergency situations, you may defer giving the Notice and obtaining an acknowledgment until the patient's medical condition permits.

All new patients seen after April 14, 2003, must receive a copy of the Notice at their first office visit. In addition, you must make the Notice available to any person who asks for it. If you revise or update the Notice with a material change, you must re-distribute the Notice to

all patients. If the revision or update is non-material, provide the new Notice to all new patients at the first date of service and to current patients only upon request.

In addition, you must post the Notice of Privacy Practices in a prominent location in your office (e.g. a copy on a stand on a desk in your office waiting room) and on your website if you have a practice website.

What happens if my patient refuses to sign the acknowledgment form?

Patient refusal to sign the acknowledgment form is NOT a bar to treatment. Simply make a notation in the patient's file that you used your best efforts to obtain an acknowledgment, but were not able to do so.

Should I distribute my Notice of Privacy Practices to patients I see at a hospital or clinic?

If you are an employee of a hospital, nursing home or clinic, you are not required to provide a copy of your own Notice to patients you treat as an employee. If you are a member of a medical staff at a facility (including voluntary, unsalaried positions), you are not required to provide your Notice to the patients you see at the hospital as long as you are covered by the institution's Medical Staff Bylaws. All physicians covered under the Medical Staff Bylaws are considered to be a member of the hospital's workforce, i.e. an employee, and are not required to provide a separate Notice of Privacy Practices (the hospital will have already provided the patient with its own Notice upon admission). If you are not sure whether you are covered under an institution's Medical Staff Bylaws, please contact that institution's Privacy Officer.

What information must the Notice of Privacy Practices contain?

The Notice required by the Privacy Rule must contain at least the following information:

1. A heading that reads: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE READ IT CAREFULLY."

2. A description, including at least one example, of the types of uses and disclosures that you are permitted to make under the Privacy Rule for treatment, payment and health care operations.

3. A description of each of the other purposes for which you are permitted or required by the Privacy Rule to use or disclose identifiable health information without the individual's consent or authorization.

4. A description of any other applicable laws that may prohibit or limit uses and disclosures that would be permitted under the Privacy Rule.

5. If you elect to make more limited uses and disclosures than those permitted by the Privacy Rule, then you should describe those more limited uses or disclosures.

6. A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke that authorization.

7. A statement of the individual's rights with respect to identifiable health information and a brief description of how those rights may be exercised.

8. A statement that you are required by law to maintain the privacy of identifiable health information and to provide individuals with notice of your legal duties and privacy practices.

9. A statement that individuals who feel that you have violated their privacy rights may complain to you and to HHS, how they may file a complaint with you, and that there will be no retaliation for filing a complaint.

Under the Privacy Rule, your notice of privacy practices must incorporate provisions in your state law, ethical standards and your privacy practices that are more protective of privacy or provide greater access to health information. For assistance in preparing your notice, you should consider consulting with your local medical or specialty association or a local attorney.

VII. MINIMUM NECESSARY STANDARD AND INCIDENTAL DISCLOSURES

What is the minimum necessary standard?

When using, disclosing or requesting protected health information, the Privacy Rule provides that a covered entity must use, disclose or request only the minimum necessary amount of information. The term minimum necessary means the least amount of information required to achieve the purpose of the use, disclosure or request.

The minimum necessary standard applies generally to uses and disclosures of identifiable health information that are permitted under the Privacy Rule. The standard, however, does not apply to:

(1) disclosures to or requests by a health care provider for treatment,
(2) disclosures made to the individual,
(3) uses or disclosures made based on an authorization given by the individual,
(4) disclosures made to HHS for enforcement of the Rule, or
(5) uses and disclosures required by law.

As you can see, the minimum necessary standard provides no restriction on the health information that may be used or disclosed to health care providers (such as physicians or laboratories) for the purposes of treating the patient.

The minimum necessary standard may prove helpful to mental health practitioners who seek to limit the amount of patient information they provide to third party payers and particularly,

to managed care companies. According to HHS, the intent of the minimum necessary standard is to be consistent with, and not override, professional judgment and standards. The American Psychoanalytic Association has adopted a practice guideline interpreting the minimum necessary standard under the Privacy Rule in the psychoanalytic setting that reflects the cumulative professional experience of its members with respect to the informational privacy that is essential for effective care. See **American Psychoanalytic Association, Interacting with Third Parties (Approved by Executive Council December 2001)**. APsaA also recognizes and strongly supports the position statement adopted by the American Psychiatric Association entitled "Minimum Necessary Guidelines for Third-Party Payers for Psychiatric Treatment". This guideline is available at www.psych.org

A study released by HHS indicates that there is wide disparity between psychiatrists and managed care organizations with respect to the minimum necessary information to provide insurance coverage for mental health services. HHS has indicated that the necessary amount of information will depend on the characteristics of a covered entity's business and its workforce. HHS has also indicated, however, that while a covered entity may assume that whatever information is requested by another covered entity is the minimum amount necessary, the covered entity that holds the information always retains the discretion to make its own minimum necessary determination.

Access to information by office staff must be limited to that information necessary to accomplish the task at hand. For example, bookkeeping or accounting personnel have no need to access individual health information in the course of performing their jobs, and steps should be taken to avoid such access.

What are incidental disclosures?

Incidental disclosures of health information, such as overhearing a conversation, are not a violation of the Privacy Rule as long as the provider takes reasonable efforts to safeguard and maintain the confidentiality of personal health information.

VIII. PSYCHOTHERAPY NOTES

What is the significance of psychotherapy notes under the Rule?

The classification of identifiable health information as "psychotherapy notes" under the Privacy Rule is significant for three reasons. (a) Such information is subject to special privacy protections which afford the patient greater control over when and how this information will be used and disclosed. (b) Patients may not be coerced by health plans and others to relinquish that control. (c) The provider has greater discretion to decide whether to permit this information to be inspected and copied by the patient.

The Privacy Rule provides greater privacy protections for information contained only in psychotherapy notes by requiring an authorization signed by the patient for use or disclosure of such information regardless of whether the use or disclosure is for routine or nonroutine purposes. By contrast, the Rule does not require an authorization or any other permission by the patient for the use and disclosure of other types of identifiable health information, including other types of mental health information, for routine uses and

disclosures. In other words, the Privacy Rule permits the use and disclosure of most identifiable health information without the individual's consent or authorization for routine and certain other purposes, but requires the individual's authorization for the use and disclosure of psychotherapy notes for both routine as well as nonroutine purposes.

The Rule also provides that covered entities (such as insurance plans) may not condition the provision of treatment, payment, or enrollment in a health plan, or eligibility for benefits on the patient furnishing an authorization for the use or disclosure of this information. This "conditioning rule" may prove helpful in dealing with managed care companies who will no longer be able to refuse payment if the patient refuses to release to the company information contained in psychotherapy notes.

Finally, the Privacy Rule does not require providers to grant patient access to psychotherapy notes for inspection and copying, unless such access is permitted or required by state law. In fact, in some states, patients have the right to access their entire medical record, including psychotherapy note material. For example, under New York law, patients are permitted to "inspect any patient information concerning or relating to [their] examination or treatment." This definition includes information that comes within psychotherapy notes as defined under the Privacy Rule. Therefore, in New York, patients are permitted to inspect or copy psychotherapy notes taken about them. This state law supercedes the Privacy Rule standard because the HIPAA rules provide that state law that grants patients greater rights than HIPAA remain in force.

If your state law already provides significant privacy protections for health care information, your everyday practices may be substantially the same under HIPAA. Nevertheless, the Privacy Rule mandates that providers who decide to maintain psychotherapy notes separately must obtain a signed authorization in a form that complies with the requirements of the Privacy Rule in order for the information to be used or disclosed to others. If an authorization is required, your preexisting state consent form may not be sufficient to meet all the requirements of the Rule.

The definition of psychotherapy notes contains numerous exceptions, and there are still further exceptions to the authorization requirement. In view of the limited privacy protections in the Privacy Rule for identifiable health information generally, it is important for you and your patients to understand the scope and limit of the special protections conferred on psychotherapy notes.

What are psychotherapy notes under the rule?

The Rule 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 and that are separated from the rest of the individual's medical record."

Therefore, whether a patient's health information will be subject to the heightened privacy protections for psychotherapy notes will depend upon whether you as the therapist separate

this information from the rest of the patient's medical record. (This is in contrast to the therapist-patient privilege under federal and state law that typically applies to all therapist-patient communications and can be waived only by the patient.) If you decide to keep psychotherapy notes "separate[] from the rest of the medical record," they may not be intermingled with the rest of the clinical record and may not be released along with other notes and records.

While you are not required by the Privacy Rule to treat psychotherapy notes differently than other information in the medical record, you should be aware of APsaA's ethical standards with respect to the privacy of medical records. APsaA's ethical standards state that

> A psychoanalyst must take all measures necessary to not reveal present or former patient confidences without permission, nor discuss the particularities observed or inferred about patients outside consultative, educational or scientific contexts…The psychoanalyst should take particular care that patient records and other documents are handled so as to protect patient confidentiality.
> **APsaA, Principles and Standards of Ethics for Psychoanalysts, Guiding General Principles, IV. Confidentiality**.

In view of the fact that the Rule permits covered entities to use and disclose identifiable health information without patient consent or permission even if the information was created or received prior to April 14, 2003, this information would have to be separated from the rest of the patient's medical record in order to be subject to the special protections that the Rule confers on psychotherapy notes. Any change in an existing medical record should be accomplished in accordance with procedures permitted by law.

What information does the Rule exclude from the definition of psychotherapy notes?

The Rule's definition of psychotherapy notes excludes the following: "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 Rule does not define these terms, although APsaA has requested clarification and has submitted suggested definitions to HHS in order to prevent the special protections for psychotherapy notes from being eroded by expansion of the exceptions. However, definitions of these terms were set forth in the Minimum Necessary Guidelines issued by the American Psychiatric Association. See **APA Minimum Necessary Guidelines for Third-Party Payers for Psychiatric Treatment, Administrative billing information, and Clinical information**. You may find these definitions helpful until further guidance is provided by HHS.

Keep in mind, however, that the special privacy protections, the conditioning rule and the limitations on access will apply only to information meeting the definition of psychotherapy notes, so information which has not been separated from the rest of the medical record and information falling within one or more of the exceptions to psychotherapy notes may be required by a health plan for routine purposes, subject, of course, to the minimum necessary rule.

When is authorization not required for use and disclosure of psychotherapy notes?

Psychotherapy notes may be used or disclosed **without an Authorization** in the following circumstances:

- by the health care provider in the course of treatment
- by a covered entity in training programs
- by a covered entity to defend in a legal action or other proceeding brought against them by the patient
- by a covered entity when required by HHS to determine compliance with the Rule
- by a covered entity to the extent required by law (for example, specific information required by a court order)
- by a covered entity to a health oversight agency for oversight of the originator of the note as authorized by law (for example, an audit by a state insurance department)
- by a covered entity to coroners or medical examiners for the purpose identifying a deceased individual, determining cause of death, or for other purposes authorized by law
- by a covered entity to prevent or lessen a serious and imminent threat to health or safety of a person or the public

If you decide to keep psychotherapy notes separated from the rest of the medical record, you must add specific language to your HIPAA documents, specifically the Notice of Privacy Practices and your Policies and Procedures.

IX. BUSINESS ASSOCIATES

The Privacy Rule permits covered entities to allow their business associates to make any uses and disclosures of identifiable health information that the covered entity is permitted to make, without further specific permission by the patient. The term “business associates” refers to all vendors, outside companies or consultants you do business with who may receive protected health information in the performance of their duties for you. The Rule requires you to enter into a business associate agreement with each vendor or contractor you hire.

Who is a business associate?

A "business associate" is an individual or entity that performs certain functions on behalf of a covered entity, including billing companies, practice management firms, administrative services, accounting firms, law firms, telephone answering services, computer repair services and others. Employees of your medical practice are part of your workforce and are not your business associates. Disclosures between providers for treatment purposes do not create a business associate relationship. Also, HHS is not considered to be a business associate. Janitorial, maintenance and cleaning services are not considered business associates, assuming the services they provide do not involve the use or disclosure of protected health information, and any access to such information should be incidental if at all.

What responsibilities does the business associate have with respect to protected health information it may receive?

The business associate agreement between the covered entity and the business associate must require the business associate to comply with all of the Privacy Rule requirements that apply to the covered entity.

What should the business associate agreement state?

The business associate agreement must contain certain provisions regarding each party's responsibilities with regard to the protected health information shared. Generally, the business associate is required to maintain the confidentiality of the health information and safeguard the information as would you. This agreement may be a separate agreement or part of a larger agreement that sets forth other terms of the relationship between you and your vendors. Model provisions for business associate contracts have been published by HHS and may be viewed at 67 Fed. Reg. at 53,264.

When should I enter into business associate agreements?

You must enter into business associate agreements with all of your business associates no later than **April 14, 2003.**

Exception to the rule: If you have an existing written contract with a business associate that was entered into prior to October 15, 2002, you will have up to one extra year to modify that contract or enter into a new business associate agreement - until April 14, 2004. If you modify such a contract after April 14, 2003 but before April 14, 2004, the contract must be in compliance the Privacy Rule as of the date of modification. This extension rule does not apply to oral contracts. In other words, if you have only an oral contract with one of your business associates, you cannot take advantage of the one-year extension and must enter into a valid, written business associate agreement with them on or before April 14, 2003.

What happens if my business associate violates our agreement?

If your business associate violates its obligations under the business associate contract, you can be held responsible under the Rule, but only if you had actual knowledge of the violation and failed to take certain required actions. HHS has no authority under the Rule to sanction a business associate. You are not required to monitor the activities of your business associates, but if you become aware that your business associate has violated the agreement, the Rule requires you to take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, the Rule requires you to terminate the agreement immediately or, if termination is infeasible, report the violation to HHS. In any event, the Rule requires you to mitigate any known harmful effect of a violation of the Rule or your policies and procedures, to the extent practicable.

X. DISCLAIMER

not be copied, distributed or disseminated for any purpose other than the use of our members in their private medical practices. This information is provided solely for general informational purposes and does not constitute, and should not be relied upon as, legal advice. Members should consult with attorneys to evaluate their specific circumstances and obtain customized advice. While all reasonable attempts have been made to ensure the accuracy, completeness, and timeliness of this information, APsaA disclaims any express or implied representations or warranties as to the accuracy, completeness or timeliness of this information for any purpose or suitability of this information for any particular use. Members using this information assume full responsibility for their use of it and agree that APsaA is not liable for any claim, loss or damage arising from any member's use or reliance upon this information.

Rev'd 6/11/03;7/10/03