42
HIPAA
(Health Insurance Portability and Accountability Act of 1996)

Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was passed to address concerns arising from the increasing complexity of the medical delivery system and the increasing dependence of that system on electronic communications. Although many states already had laws in place protecting patient privacy, it was felt there should be a federal standard that would establish a minimum level of protection. In cases where state laws are more stringent than HIPAA in protecting patients' records and their access to them, those state laws take precedence over HIPAA.

HIPAA mandates that the federal Department of Health and Human Services (HHS) develop rules covering the transmission and confidentiality of individually identifiable health information, with which all entities covered under HIPAA (see box below) must comply.

The first two rules finalized under HIPAA were the Transactions Rule and the Privacy Rule. The Transactions Rule is meant to facilitate the ability to transfer health information accurately and efficiently, and the Privacy Rule was created to protect the confidentiality of patient information. The third rule finalized was the Security Rule, which was created to protect the confidentiality of patient records kept on computers.

The underlying premise of the Privacy Rule is that a patient's individually identifiable health information belongs to the patient, and that the patient has the right to access that information (except in the case of psychotherapy notes, which would seem to be designated as the property of the psychotherapist who created them--see below) and to control what is done with it.

Under the Transactions Rule, the Department of Health and Human Services (HHS) created regulations that establish a uniform set of formats, code-sets, and data requirements that are intended to permit the efficient, easily transferable, and secure electronic exchange of information for all healthcare administrative and financial transactions. The agency that administers the Medicare program, the Centers for Medicare and Medicaid Services (CMS), has been charged with overseeing the implementation of the Transactions Rule. The Privacy Rule is administered by the Office for Civil Rights (OCR) at HHS**.**

The Security Rule can be seen as an extension of the privacy rule, it requires that HIPAA-covered entities "protect against any reasonably anticipated threats

or hazards to the security or integrity of protected health information, and protect against any reasonably anticipated uses and disclosures not permitted by the Privacy Rule and other more stringent laws."

Introduction

Following the publication of the Transactions Rule (Standards for Electronic Transactions) and the Privacy Rule (Standards of Privacy for Individually Identifiable Health Information), both of which fall under the Administrative Simplification part of HIPAA, there was a great deal of concern about how compliance with these rules would affect the day-to-day practice of psychiatry.

In point of fact, compliance with HIPAA should not have proven all that difficult for psychiatrists. Those who see patients under the Medicare program were already using the code-sets required by the Transactions Rule. And psychiatrists, who have always been aware of the absolute necessity for maintaining the confidentiality of their patient information, were very likely to already have in place the confidentiality safeguards required by HIPAA.

Although HIPAA is a very complex law, the steps a psychiatric practice must take to comply with its two current rules are all eminently doable and should not require excessive retooling of a practice that is already functioning properly.

Note: If your office does not participate in *any* electronic transactions and you do not have any business associates who participate in any electronic transactions on your behalf, you are not covered under HIPAA and are not required to comply with its rules. You should know, however, that if your practice has ten or more full-time employees (or the equivalent of ten full-time employees) you are required to file Medicare claims electronically unless you can establish that you have no means of doing so, which means you will have to be covered by HIPAA. Also, even if your practice is small enough to be eligible to continue filing paper claims, you will be penalized by Medicare if you fail to submit prescriptions electronically and fail to have an electronic health records system in place

The Transactions Rule

The Transactions Rule defines standards and establishes code-sets and forms to be used for electronic transactions that involve the following kinds of healthcare information:

1. Claims or Equivalent Encounter Information

2. Eligibility Inquiries
3. Referral Certification and Authorization
4. Claims Status Inquiries
5. Enrollment and Disenrollment Information
6. Payment and Remittance Advice
7. Health Plan Premium Payments
8. Coordination of Benefits

The rule also requires the use of employer and provider identification numbers. The National Provider Identifier (NPI) became available in 2006, and is supposed to have replaced all other provider identifiers, including the UPIN previously issued by Medicare. (Despite this, it should be noted that Medicare still asks for a legacy number (the UPIN, now referred to as the PTAN) for identification purposes when providers call in for assistance on provider assistance lines.)

The Transactions Rule code-sets replaced the approximately four hundred different formats that had been in use for healthcare claims processing. The code-sets required under the Transactions Rule are:

- **Procedure Codes**: AMA CPT (Current Procedural Terminology) and HCPCs (Healthcare Common Procedure Coding System) codes
- **Diagnosis Codes**: ICD-9 CM (International Classification of Diseases, 9th Revision, Clinical Modification) codes [**note**: As of October 1, 2013, ICD-10 codes must be used on all HIPAA transactions. It's codes should coincide with the codes in the DSM-IV and V.]
- **Drugs and Biologicals**: NDCs (National Drug Codes)
- **Dental Codes**: Code on Dental Procedures and Nomenclature for Dental Services

The Privacy Rule

The Privacy Rule went into effect on April 14, 2003. It was enacted to address public concerns that the increased use of electronic technology and changes in the way healthcare is delivered were undermining the confidentiality of the individually identifiable health information maintained and shared by physicians, health plans, and the other entities involved in patient care (however peripherally). The Privacy Rule establishes a federal floor of standards for the use and disclosure of patient information. Many states had already passed legislation to deal with this issue, and in cases where the state law is more stringently protective of patients' rights, the state laws take precedence over the federal Privacy Rule. Contact your state medical society to find out whether there are state laws that preempt HIPAA in your jurisdiction.

Patients' Rights

Under the Privacy Rule your patients have statutory rights regarding their individually identifiable health information:

- You must give your patients written notice of their privacy rights and the privacy policies of your practice, how you will use, keep, and disclose their health information; and you must make a good faith effort to obtain your patients' written acknowledgment that they have seen this notice.
- Patients must be able to get copies of their medical records and request amendments to those records within a stated time frame (usually 30 days). Patients do not have the right to see psychotherapy notes (see below for definition).
- Upon request, you must provide your patients with a history of most disclosures of their medical records (there are some exceptions)
- You must obtain your patients' specific authorization for disclosures of their information other than for treatment, payment, and healthcare operations (these three are considered to be "routine" uses). [**note:** Although HIPAA does not require that you obtain your patients' consent before disclosing their health information for treatment, payment, and healthcare operations, psychiatric ethics demand that you obtain written consent for these releases as well.]
- Patients may request alternative means of communication of their protected information, i.e., they may ask that you only contact them at a specific address or phone number.
- You generally cannot condition treatment of patients on obtaining their authorization for disclosure of their information for nonroutine uses
- Your patients are authorized to complain about violations of the Privacy Rule to you, their health plan, or to the Secretary of HHS

Psychotherapy Notes

The writers of the Privacy Rule acknowledged that psychotherapy notes should be subject to a more stringent standard of confidentiality than other medical records. Psychotherapy notes are the only part of their files patients do not have access to. According to the rule, *psychotherapy notes* are specifically defined as the notes taken by a psychotherapist "documenting or analyzing the contents of a 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." Essentially, psychotherapy notes are the notations kept during therapy sessions that deal with the patient's personal life and the psychiatrist's reactions, rather than with the patient's disorder. It is vital to understand that psychotherapy notes must be kept separate from the rest of the medical record (i.e., on a different sheet of paper) if they are to be protected as a separate entity.

It is important to be clear about the definition of psychotherapy notes under HIPAA. Psychotherapy notes do **not** include references to medication prescribing

and monitoring; session start and stop times; modality and frequency of treatment furnished; results of clinical tests; or any summary of the following items: diagnosis, symptoms, functional status; treatment plan; progress to date; and prognosis. All of this information is part of the medical record.

Minimum Necessary

The concept of minimum necessary disclosure is the rule for all routine disclosures of patients' individually identifiable information under HIPAA. However, when a patient gives authorization for a specific nonroutine disclosure, minimum necessary does not apply.

What a Physician's Office Must Do to Comply with the Privacy Rule

To be in compliance with HIPAA, every practice must:

- Have written privacy procedures that include administrative, physical, and technical safeguards establishing who has access to individually identifiable patient information, how this information is used within the practice, and when the information will and will not be disclosed to others.
- Ensure its business associates protect the privacy of health information.
- Train employees to comply with the Privacy Rule
- Designate a person to serve as a privacy officer (this can be the psychiatrist if you are in a solo practice)
- Establish grievance procedures for patients who wish to inquire or complain about the privacy of their records.

The Security Rule

According to malpractice experts, the Security Rule's requirements should be viewed as a standard for the protection of electronic health information, which all providers, even those not covered by HIPAA can be expected to meet or exceed. The Security Rule does not set forth any specific technology to be used to protect electronically maintained health information, it rather demands that protections be in place against *reasonably anticipated,* breaches of security. Most commercially available electronic health record systems should enable compliance with the HIPAA Security Rule

An in-depth discussion of HIPAA prepared for APA members can be found on the APA website at http://www.psychiatry.org/practice/managing-a-practice/hipaa .