

HIPAA

*what you need to know now*

# The Privacy Rule

*A primer for psychologists*

Updated 2009

PRACTICE  CENTRAL

This publication answers basic questions that psychologists often ask about the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

This publication was originally prepared in March 2002 by the APA Practice Organization (APAPO) and the APA Insurance Trust (the Trust). The APAPO and the Trust have updated and simplified the information in light of several years of experience with answering members' questions about the HIPAA Privacy Rule.

Although the content is primarily applicable to psychologists in private practice, psychologists who work in other settings such as hospitals, integrated delivery systems, and clinics also should find it useful.

## Section A. WHAT IS THE PRIVACY RULE?

The Privacy Rule is a federal regulation under the HIPAA statute that sets minimum standards for your disclosure of patient information to third parties:

- Under what circumstances you can disclose patient information
- What kind of consent is needed to disclose patient information and from whom
- When no consent is required to disclose patient information
- What is the appropriate scope of patient information you can disclose

It also increases patients' rights regarding their health information. Among other things, the Privacy Rule gives patients the right to:

- Receive notice from you describing how and when you will disclose the patient's information
- Access their health information (with certain limitations)
- Amend their records

As described below, the Privacy Rule does not preempt, or override, state privacy law provisions that give greater privacy protection, or that give the patients greater access rights than the Privacy Rule. Thus, in each state HIPAA compliance requires that you must comply with a mixture of state law and the federal Privacy Rule.

## Section B. DO I NEED TO COMPLY WITH THE PRIVACY RULE?

For most psychologists, triggering the need to comply with HIPAA and the Privacy Rule occurs when they do all of the following:

- 1) Electronically transmit
- 2) Protected Health Information (PHI)
- 3) in connection with insurance claims or other third-party reimbursement.

These three elements are described in this primer.

Less frequently, psychologists trigger HIPAA and the Privacy Rule by electronic transmission of PHI in connection with other transactions specified by the Privacy Rule.

For additional information see *Appendix A: "What Triggers the Need to Comply?"* an article from the Winter 2007 issue of Good Practice magazine from the APA Practice Organization.

Electronic submissions of PHI that are not in connection with one of these transactions will not trigger HIPAA (for example, e-mailing records to another psychologist for a consultation).

If someone acting on your behalf, such as a billing service, electronically submits PHI (in connection with a specified transaction), this action will trigger HIPAA and compliance with the Privacy Rule will be required.

Once triggered, the Privacy Rule applies to all of the PHI in your entire practice, not just to the information in electronic form and not just the professional services that triggered the Rule. For example, you may have triggered the Rule by an electronic transmission to an insurance company related to the portion of your practice involving psychotherapy. Once the Rule is triggered, however, it will also apply to the other parts of your practice, for example, your involvement with disability evaluations. The Privacy Rule does not appear to permit an individual practitioner to segregate out one portion of his or her practice as being subject to Rule and another portion as not subject to the Rule. In the example above, you could not say that only the psychotherapy portion of your practice needs to be compliant, but not the disability evaluation portion of your practice.

It is theoretically possible for you not to trigger HIPAA if you do not transmit patient information electronically or have a billing service transmit it for you. However, the health care delivery system is becoming increasingly electronic and, therefore, we recommend that all psychologists, particularly those earlier in their careers, make their practices compliant with HIPAA. By doing so, you will make sure any future actions you may take do not place you in violation of the Privacy Rule. For example, you may decide at some point to accept an interesting case where the patient's payor requires you to bill electronically. If so, you will be required to come into compliance immediately and will not be given any grace period for meeting all of the HIPAA requirements.

### What is an electronic transmission?

The most common form of electronic transmission for psychologists is via the Internet (for example, sending email to an insurance company or making transactions on an insurance company Web site). Electronic transmission also includes: the 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.

Sending paper faxes (where you put a piece of paper into a fax machine in order to send it) are not considered electronic submissions. However, computer-generated faxes (where a document is already in electronic form and faxed directly from a computer) are considered electronic submissions.

### What is PHI?

The Privacy Rule applies to protected health information (PHI). The Rule defines PHI as:

- Information that relates to: the past, present or future physical or mental health condition of a patient; providing health care to a patient; **or** the past, present, or future payment for the patient's health care;
- That identifies the patient or could reasonably be used to identify the patient; **and**
- That is transmitted or maintained in any form or medium.

Health information is not considered PHI if it does not identify a patient and provides no reasonable basis for identifying a patient.

PHI also excludes educational records covered by the Family and Educational Right and Privacy Act (FERPA).

### Who else must comply with the Privacy Rule?

In addition to understanding whether you need to comply with HIPAA, it is helpful to understand who else in the health care arena must comply. The HIPAA Privacy Rule applies to "covered entities" including:

- Health care providers (who transmit PHI electronically in connection with the specified transactions, as described above)
- Health plans (including employer-sponsored group plans, Medicaid, Medicare, etc.). For example, virtually all health insurers must comply with HIPAA. However, other types of insurers, such as life and disability insurers, do not have to comply.
- Health care clearing houses<sup>1</sup>

In a different and indirect way, the Privacy Rule also applies to people and companies that handle PHI when performing services for covered entities, such as billing services and accountants. These people or companies are called "business associates" and their role under the Rule is described below.

## Section C. WHAT DO I NEED TO DO TO COMPLY WITH THE RULE?

In general, the Privacy Rule requires psychologists to:

- Understand the basic Privacy Rule requirements and how they interact with state privacy laws (as described below)
- Provide a notice and other information to patients about their privacy rights and how that information can be used
- Use other required forms, such as authorization forms, for releasing information.
- Adopt clear privacy procedures for their practices
- Train employees so that they understand privacy procedures
- Designate an individual to be responsible for seeing that privacy procedures are adopted and followed

<sup>1</sup> A health care clearinghouse is a public or private entity that: converts or assists with the process of converting health information into standardized HIPAA-compliant data or a standard transaction; and/or receives a standard transaction and converts or assists with the process of converting that standard transaction back into a non-standard format or non-standard data for the receiving entity.

- Have a business associate contract with outside entities who handle PHI (for example, billing services and accountants)
- Secure patient records

See Section H for further details.

In February 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act became law as part of the economic stimulus package passed by Congress. This law is likely to change the way you must comply with the HIPAA Privacy Rule in the future. We anticipate that the U.S. Department of Health and Human Services will begin developing regulations to implement the law late in 2009. Check for updates concerning the HITECH law online at [APApractice.org](http://APApractice.org) or [apait.org](http://apait.org).

### Preemption: Interaction with State Law

The HIPAA Privacy Rule is meant to provide patients with a *minimum* level of privacy protection. Thus, it only takes precedence over provisions of state laws that provide less privacy protection or that provide patients with less access to and control over their health information. Conversely, the Privacy Rule does **not** preempt state law provisions that give patients greater privacy protection from third parties or that give patients greater access to and control over their records. We refer to both types of state laws as being “more stringent” than the Privacy Rule. However, the Privacy Rule specifically does not preempt a narrow range of state laws, such as laws giving or denying parents access to their childrens’ records, regardless of how stringent they are.

The result of the complicated preemption analysis is that the law you must follow is a mixture of Privacy Rule and state privacy law provisions.

### Section D. HOW CAN I GET HELP WITH COMPLIANCE?

There are a number of compliance products available for health care providers. The Practice Organization and the Trust spent thousands of attorney and psychologist hours developing a compliance product designed for psychologists with solo or small group practices: *HIPAA for Psychologists*. It is the only product we are aware of that provides a preemption analysis for all 50 states (as well as the District of Columbia

and three territories) of the privacy laws that affect psychologists.<sup>2</sup> That analysis is incorporated into state-specific forms for you to use in your practice.

*HIPAA for Psychologists*, offered as an online course at **APApractice.org**, includes:

- A step-by-step guide to becoming compliant with the HIPAA Privacy Rule
- A variety of state-specific forms that you can customize for your practice, including a notice of privacy practices, authorization forms, and a psychotherapist-patient agreement;
- Policies and procedures
- A detailed explanation of how the Privacy Rule interacts with your state’s law, and
- The opportunity to earn Continuing Education credits.

### Section E. WHAT ARE THE BASIC RULES ON RELEASING PATIENT INFORMATION?

It is important to understand when you can release PHI with patient consent, when an authorization is required, and when you can release PHI with neither consent nor authorization.

Consent is a general agreement by the patient, typically signed at the start of treatment or when the patient applies for health insurance. It covers a variety of anticipated releases of PHI. Authorization, by contrast, is a detailed form that is signed contemporaneously and describes in detail what information will be released to whom, for what purposes, in what time frame and under what conditions. Those requirements are detailed below.

#### 1. Consent

The Privacy Rule does not require consent or authorization for releases of PHI in connection with routine releases for treatment, payment, and health care operations purposes as defined below (once your patient has effectively accepted your notice of privacy practices as described below).

However, most, if not all, states have consent requirements laws that apply, and several jurisdictions such as California and the District of Columbia have authorization requirements.

<sup>2</sup> There are other HIPAA compliance products available for purchase, but neither the APA Practice Organization nor the APA Insurance Trust can speak to their quality or legal accuracy.

Many states have exceptions to consent (or authorization), such as for consultations regarding the patient's treatment, or for payment purposes. The bottom line is that psychologists face the complex matter of complying with both the Privacy Rule and state law. You must obtain all of the required consents and authorizations before disclosing PHI.

## 2. Definitions

**Treatment:** This is 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 your activities to obtain reimbursement for health care services. These activities can include: 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, auditing functions, business planning and administrative services.

The "treatment, payment, and health care operations" exception applies when you are releasing information for:

- Your treatment, payment and health care operations
- For the treatment activities of another health care provider
- For the payment activities of the covered entity that receives the information
- In certain circumstances, for the health care operations activities of the covered entity receiving the information (This provision typically covers audits by health insurers.)

## 3. Authorization

You must obtain the patient's authorization before releasing PHI for purposes other than treatment, payment, or health care operations. For example, if you receive a request for information from an employer or school that is not part of the billing procedures or claims process, you cannot release it without patient authorization.

You must also obtain an authorization before releasing

psychotherapy 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 describe the following:

- Exactly what information will be disclosed
- To whom the information will be disclosed
- The purpose of the disclosure
- An expiration date
- The right to revoke the authorization under the Privacy Rule or state law, whichever gives the patient more rights
- That information disclosed may be subject to redisclosure by the recipient and is no longer protected by the HIPAA Privacy Rule.
- The limited conditions under which you may require a patient to sign the authorization before providing services.

An authorization to release psychotherapy notes must be separate from the authorization to release the rest of the patient's record.

## What are psychotherapy notes?

The Privacy Rule's definition of psychotherapy notes has the following elements:

- 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,
- That are separated from the rest of the patient's medical record.

The definition in the Privacy Rule specifically excludes the following:

- The modalities and frequencies of treatment furnished
- Results of clinical tests
- Any summary of the following items: diagnosis; functional status; the treatment plan; symptoms; prognosis and progress to date
- Counseling session start and stop times
- Medication prescription and monitoring

The Privacy Rule does not mandate what you must put in your patient records. Nor does it require you to keep psychotherapy notes. However, the Privacy Rule does confer heightened privacy protection when you keep psychotherapy notes that are separate from the rest of the clinical record.

The rationale for special psychotherapy notes protection is that such notes reflect communications whose confidentiality is essential to successful psychotherapy, and that these notes serve as the therapist's private notes for his or her own use. As such, they are not needed by, and do not need to be shared with, others in the health care delivery system such as third party payers and other health care professionals.

For practical information on keeping psychotherapy notes, such as what information may be placed there, and what it means for the record to be separate, see **Appendix B** for a related article, "Practitioners: Take Note," from the Practice Organization's Winter 2007 issue of Good Practice magazine.

### Can health insurers ask for psychotherapy notes?

A covered entity (for example, a managed care or health insurance company, or an employee benefit plan) is prohibited from demanding that a patient execute an authorization as a condition for treatment, eligibility for benefits, or payment of claims. (However, health insurers can make such a demand when determining whether your patient is eligible for coverage when they first apply for such insurance.) Further, companies cannot require you to turn over psychotherapy notes during an audit of your patient records. This eliminates one of the biggest complaints from practitioners and consumers about intrusive requests for information from managed care companies. (Remember that life, disability and workers comp insurers are not covered by HIPAA and can demand that the patient execute an authorization to release your psychotherapy notes.)

However, insurers can refuse to pay for services if you have not sufficiently documented medical necessity in the clinical record (the part of the record separate from the psychotherapy notes) or other information sent to the company. You should be able to provide an adequate rationale for medical necessity of the treatment provided in your clinical record.

### When can you disclose PHI without consent or authorization?

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

following purposes:

- To show compliance with the Privacy Rule
- When required by law
- For health oversight activities of the originator or the psychotherapy notes
- To a coroner or medical examiner for identification, cause of death, or other duties authorized by law
- To avert a serious threat to the health or safety of a person or the public (explained in detail later in this document)
- 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 certain purposes related to:

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

### 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 (for example, a billing clerk may have access only 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 (many states require patient consent) to disclose PHI for treatment purposes only to another provider.
- Minimum necessary disclosure does not apply to requests for information that require authorization, such as with psychotherapy notes because the information to be disclosed is specifically described by the authorization itself.

## Section F. WHAT RIGHTS DOES THE PRIVACY RULE GIVE PATIENTS?

---

### Notice

Under the Privacy Rule, patients have the right to receive a notice informing them about potential uses and disclosures of their PHI and their right to limit those uses and disclosures.

You will normally give the patient your notice form at the first session and ask him or her to sign an acknowledgement that he/she received the notice. However, if the patient refuses to sign the acknowledgement, it is sufficient to note in your records that you asked the patient to sign and he/she refused.

### Patient Access To Records

Under the Privacy Rule, a patient is allowed to inspect and obtain a copy of his or her records with limited exceptions. You can require that the request be made in writing. Generally, you must fulfill the request within 30 days.

Under the Privacy Rule, 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

You may also withhold records if you have safety concerns -- for example, when you determine, in the exercise of professional judgment, that giving access to records is reasonably likely to endanger the life or physical safety of the patient or another person.

However, most states have laws that give patients greater access to their records than the Privacy Rule, at least in some respects. Therefore, patient access will be determined by the preemption analysis of state law and the Privacy Rule provisions.

### Patient Amendment of Records

The Privacy Rule gives patients a right to request additions to (but not deletions from) their records if they feel that the information is incorrect. If you did not create the records at issue, you generally do not have to honor a request to amend -- unless the person who created the record is no longer available to act on the request.

## Accounting for Disclosures

The Privacy Rule gives the patient a right to receive an accounting of disclosures of PHI that you made over the prior six years without needing consent or authorization as described in Section E above, for example, disclosures required by law and abuse reporting.

## Section G. SPECIFIC SITUATIONS UNDER THE PRIVACY RULE

---

### 1. Dealing with the Judicial System and Administrative Proceedings

As a result of statutes in virtually all states protecting psychotherapist-patient communications, information acquired in the course of the psychotherapy relationship cannot be disclosed without a HIPAA-compliant authorization signed by the patient or a court order. These state privilege laws take precedence over the less protective Privacy Rule provisions concerning subpoenas.

For more information on responding to subpoenas, see *Appendix C*, “How to Deal with a Subpoena.”

### 2. Disclosures to Avert A Serious Threat to Health or Safety

Consistent with applicable law and professional ethics, you may disclose PHI without consent or authorization to prevent or lessen a serious and imminent threat to the health or safety of a person (including the patient) or the public. You can only disclose to people 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 “duty to warn” laws based on the seminal Tarasoff case from California.

The U.S. Department of Health & Human Services (HHS), which promulgated the Privacy Rule and enforces it, intended this disclosure to be very narrow and to apply only in “rare circumstances.” It did not intend to create a “duty to warn” beyond the existing duty under state law.

The Privacy Rule also permits disclosure in situations in which a patient admits to participating in a violent crime, although such statements made in the course of psychotherapy are typically prohibited from disclosure by state law. This provision would apply only in the rarest of circumstances.

### 3. Legal Representatives of Adult Patients

You must generally treat a personal or legal representative (such as a guardian) of an adult or emancipated minor patient as if he or she were the patient, in terms of letting them exercise the privacy rights described above – for example, the right to access records or authorize disclosures to third parties.

You may refuse to let the guardian or other representative of the patient exercise the patient's privacy rights under the following conditions:

- If you have 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 letting the representative exercise the patient's privacy rights could endanger the patient; and
- You decide "in the exercise of professional judgment" that letting the representative exercise those rights is not in the best interest of the patient.

### 4. Minors

The Privacy Rule indicates that parents generally have the authority to make health care decisions about their minor children. Thus, parents are generally recognized as personal representatives and can therefore access PHI about their children, authorize disclosures to third parties<sup>3</sup> and exercise other privacy rights of the child. The three exceptions to this provision are:

- 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 or guardian assents to an agreement of confidentiality between you and the minor

If one of these exceptions applies, the Privacy Rule makes it clear that, although records do not have to be disclosed, the minor may still voluntarily choose to involve a parent or adult as a personal representative. 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.

In addition, regardless of the information above, the Rule specifically does not preempt state laws that either grant or deny parents access to their children's health information.

Finally, you may refuse to let the parent or guardian exercise the minor's privacy rights under the following conditions:

- If you have reason to believe that the minor has been or may have been subjected to domestic violence, abuse or neglect; or there is reason to believe that letting the parent or guardian exercise the minor's privacy rights could endanger the minor; and
- You decide "in the exercise of professional judgment" that letting the parent or guardian exercise those rights is not in the best interest of the minor.

### 5. Business Associates

A "business associate" is an organization or person outside of your practice to whom you send PHI so that they can provide services to you or on your behalf (for example, accountant, lawyer, billing service, collection agency). A business associate is not considered a covered entity that must comply directly with HIPAA.

A business associate relationship is not created when you:

- Disclose PHI within a covered entity (such as within your own practice)
- Disclose PHI for purposes related to treatment
- Disclose PHI to federal oversight health agencies such as the Medicare Peer Review Organization

You may disclose PHI to a business associate as long as you have a business associate contract under which the business associate promises to 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, you will need to contractually obligate the business associate to follow all the HIPAA compliance requirements that you are required to follow.

<sup>3</sup> The Privacy Rule clarifies that when a parent, guardian, or other legal representative for a child or minor signs an authorization for the release of records, the authorization remains valid until it is revoked or expires even after the child becomes an adult.

Once a business associate contract is in place, you must monitor the contract to ensure that the business associate is complying. If you know that the business associate is breaching or violating his or her obligation under the contract, you have to take reasonable steps to cure the breach. If those steps are unsuccessful, you may have to terminate the contract and/or report the problem to HHS.

## Can I disclose to law enforcement agencies?

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

- A) As required by law, or
- B) 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 from a government agency, including an administrative subpoena or summons, civil or authorized investigative demand or similar process authorized by law. For administrative requests, the following conditions must be met:
    - The information 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
    - The agency could not reasonably use de-identified information (the data must not reveal the patient's identity).

## Section H. WHAT STEPS WILL I NEED TO TAKE?

Following is an overview of the types of administrative processes you are expected to implement in order to meet the requirements of the HIPAA Privacy Rule. It also describes the resources available in *HIPAA for Psychologists* to assist you with compliance.

### Learn about the Privacy Rule

You must learn how the Privacy Rule, in combination with state law, governs your handling and disclosure of records, as well as the legal meaning of Privacy Rule terms such as "authorization" and "psychotherapy notes."

### Implement policies and procedures

You must implement office policies and procedures with respect to PHI to comply with the requirements of the Privacy Rule.

### Put administrative and physical safeguards in place.

Appropriate administrative, technical and physical safeguards must be in place to protect the privacy of PHI.

### Appoint a Privacy Officer.

You must designate someone to be responsible for seeing that privacy procedures are adopted and followed. In solo and small practices, the privacy officer can be you or another psychologist.

### Provide a Notice Of Privacy Practices.

You must have a notice of privacy practices that outlines potential disclosures and patient's privacy rights as required by the Rule. You must provide a copy of this notice to your patients.

### Train your workforce.

You must train all members of your workforce 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.

### Possess and apply sanctions.

You must have and apply appropriate sanctions against members of your 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.

### Implement a compliant process.

As part of your required policies and procedures, you need a process for responding to patient complaints about non-compliance with the Privacy Rule or non-compliance with your Privacy Rule policies and procedures.

## Document compliance procedures

You must maintain policies and procedures in either electronic or paper format. You must maintain the various types of documentation required by the Privacy Rule for six years from the date of creation or the date when the document was last in effect, whichever is later.

**Note:** A common source of confusion is whether the Privacy Rule dictates how long you must keep your clinical records. The Privacy Rule's recordkeeping requirement applies only to the documentation that the Privacy Rule requires. It does not determine how long you must keep your clinical record, which is generally determined by state recordkeeping laws. For further information, see the Record Keeping Guidelines on [APApractice.org/practice-central](http://APApractice.org/practice-central).

## Duty to mitigate.

You must mitigate, to the extent practical, any known harmful effect of improper disclosures of PHI that violate the Privacy Rule by yourself, your employees, or your business associates. For example, if your receptionist inadvertently sends the wrong patient records to an insurer for reimbursement, you might be required to request the records back and inform the patient of the error.

## Section I. WHAT IS THE HISTORY AND BACKGROUND OF HIPAA?

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

The act was designed to protect Americans who have pre-existing illnesses or medical conditions from losing their health insurance when they changed jobs or residences. The law also was intended to streamline the health care system through the adoption of consistent standards for transmitting uniform electronic health care claims. Making the law work necessitated adopting standards for securing the transmission and storage of patient information and for protecting a patient's privacy. Privacy risks were increased by encouraging electronic transmission and storage of patient records. For example, while it takes considerable effort to improperly copy and distribute copies of patients' paper records, electronic records can be widely disseminated with a few clicks of a computer mouse.

## Additional Resources

Numerous resources are available from the APA Practice Organization at [APApractice.org](http://APApractice.org).

**Revised and Updated February 2009**