

Reducing Risk

A Publication on HealthCare Risk Management from Princeton Insurance

HIPAA Privacy Rule

Background

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) was enacted by Congress in part to address the need for national standards to protect the privacy of medical records and other personal health information.

HIPAA authorized the Department of Health and Human Services (“HHS”) to establish regulations to protect the security and privacy of **protected health information** (“PHI”). PHI includes information in medical records and other individually identifiable health information that either identifies an individual—or “there is reasonable basis to believe” can be used to identify the individual—that is maintained, received or transmitted in any form or medium, including written, electronic and oral, by a HIPAA covered entity.

A HIPAA covered entity is a physician practice or any other healthcare provider that electronically transmits healthcare information including claims, referrals and health plan eligibility or enrollment, or has another entity do so on its behalf. Health plans and healthcare clearinghouses are also HIPAA covered entities.

The regulations for privacy and confidentiality of PHI are known as the Privacy Rule. The Privacy Rule went into effect on April 14, 2003. All covered entity healthcare providers, including medical and dental practitioners, are required to comply with the Privacy Rule.

It is important to note that the privacy regulations state what must be done, not how to accomplish it. A “reasonableness” standard pervades, giving covered entities flexibility to design policies and procedures suitable for their size and needs to meet the standards. Also, HIPAA will be an ongoing factor in healthcare practice that will continue to evolve.

A physician or dental practice must assess its privacy practices on an ongoing basis and revise them as needed to remain in compliance with HIPAA. The following provides a brief overview of the regulations and some general office practice guidelines.

HIPAA Privacy Principles

The privacy principles outline the basic components and intent of HIPAA:

- **Consumer Control** — provides consumers with new rights to understand and control how their PHI is used
- **Boundaries on Use and Disclosure of PHI** — limits the use and disclosure of PHI to the minimum amount necessary to meet the purpose and requires authorization for use or disclosure of PHI that is requested for non-health purposes
 - **Use** — the sharing, employment, application, utilization, examination or analysis of PHI within the covered entity's practice
 - **Disclosure** — the release, transfer, provision of access to, or the divulging of PHI to someone outside the practice
- **Ensure Security of PHI** — requires covered entities to adopt written privacy policies and procedures
- **Establish Accountability** — provides for civil and/or criminal penalties for covered entities that violate a patient's privacy rights
- **Balance Public Responsibility with Privacy Protections** — allows disclosures of PHI without patient authorization for certain public needs such as reporting of diseases or abuse

Consumer Rights

This federal legislation grants consumers the legal right to:

- Be informed about the provider's privacy practices
- Inspect and copy their medical records
- Request amendments and corrections to their medical records
- Restrict disclosures of their PHI
- Obtain an accounting of all non-routine uses and disclosures of PHI
- Complain to the office practice and HHS about any Privacy Rule violations

What You Need to Know and Do to Comply with HIPAA

HIPAA and State Laws

The Privacy Rule is intended to enhance the privacy protections that many existing state laws already provide. A state or federal law that is “more stringent” than HIPAA i.e., offers stronger privacy protections than HIPAA, continues to apply. Additionally, laws that regulate controlled substances, or pertain to required reporting and to licensure or certification of individuals or facilities, still apply.

Minimum Necessary Standard

The “minimum necessary” provision requires covered entities to make reasonable efforts to limit the use and disclosure of, and requests for, PHI to the *minimum necessary* to meet the intended purpose of the request. Covered entities are permitted to make their own determination of what PHI is reasonably necessary for a particular purpose. The minimum necessary standard does not apply to disclosures to other healthcare providers for treatment purposes or to disclosures made pursuant to a valid authorization as discussed below.

The Privacy Rule permits incidental disclosures of PHI that result from a permitted use or disclosure as long as the provider takes appropriate and “reasonable safeguards” to protect against inadvertent disclosure, e.g., discussing a patient’s care in a separate area of office, speaking in “hushed tones.” However, *erroneous or careless disclosures are not excused*. Using office sign-in sheets that do not display medical information and calling out names in a waiting area are permitted.

To comply with the “minimum necessary” standard, a physician’s office must:

- ✓ Make “reasonable efforts” to limit the use and disclosure of PHI to the “minimum necessary to accomplish the intended purpose” of a request for PHI
- ✓ Have policies and procedures for its business practices that reasonably minimize the amount of PHI used, disclosed, and requested, and limit access to PHI.

Notice of Privacy Practices

Physician offices must give their patients a written notice of privacy practices that informs patients about their privacy rights and the office’s privacy practices. The notice must be given to all patients before or at their initial encounter and anytime thereafter upon request.

Providers are required to make a good faith effort to obtain the patient’s written acknowledgment of receipt of their notice of privacy practices. The form of the acknowledgment used is discretionary and may be as simple as having the patient date and sign or initial the cover page of the notice.

Written acknowledgment of the patient’s receipt of the notice of privacy practices is *not* a prerequisite for treating a patient. However, if a signed acknowledgment is not obtained, the attempt and the reason it was not obtained must be documented in the medical record.

Reducing Risk

Uses and disclosures of PHI for the treatment, payment, and healthcare operations (“TPO”) of your practice must conform to your notice of privacy practices and are permitted even if a patient refuses to give an acknowledgment. Uses and disclosures of PHI for non-TPO purposes require a signed authorization form as discussed below.

Many websites for healthcare providers have sample notices of privacy practices, including the Medical Society of New Jersey at www.msnj.org, which makes HIPAA materials available to its members. Attorney review of your practice’s Notice of Privacy Practices for HIPAA compliance is always advisable.

Authorizations

A signed authorization must be obtained before PHI is used or disclosed for any purpose other than TPO, such as releasing information for a life insurance application or for use in marketing. A provider may not refuse to treat a patient who does not give authorization. A copy of all signed authorizations must be maintained in order to document the practice’s uses and disclosure of PHI. Patients are permitted to request an accounting of non-routine uses and disclosures of their PHI that they have not authorized for the six years prior to the date that they make a request for an accounting.

The privacy regulations require specific elements in an authorization form:

- ✓ A description of the PHI to be used or disclosed by the covered entity
- ✓ The person who is authorized to use or disclose the PHI
- ✓ The person to whom the PHI is to be disclosed
- ✓ The purpose for the requested use or disclosure
- ✓ The date or a specified event on which the authorization will expire
- ✓ Statement that the individual has the right to revoke the authorization in writing and a description of how the authorization may be revoked
- ✓ Statement that the PHI disclosed in accordance with the authorization may possibly be redisclosed by the recipient and no longer protected by the privacy rule regulations
- ✓ Statement that the patient may not be required to sign an authorization in order to receive treatment or coverage.
- ✓ The date and signature of the patient or the patient’s authorized representative with a description of the representative’s authority to act on behalf of the patient.

Psychotherapy Notes Exception

Psychotherapy *notes* must be separated from the rest of a patient's medical record. Release of psychotherapy notes for *any* purpose, including treatment, payment, or healthcare operations (TPO), requires a separate authorization. Patients do not have the right to read and copy or request amendments to psychotherapy notes in their medical records unless the record is involved in litigation by the patient.

PHI of Minors

State law, including statutes, regulations and case law, governs disclosures of a minor's PHI to parents. For legal advice regarding a specific law, consult a qualified attorney.

Patient Requests for PHI

Patients have the right to inspect and obtain a copy of their PHI for as long as the provider maintains the information. A physician may only deny a patient access to the information if he/she believes that it would endanger the patient's life or safety. A patient who is denied access must be given the opportunity to have the reason for the denial reviewed by a healthcare professional who was not involved in the initial decision to deny access.

The requested information must be provided to the patient within thirty (30) days if it is stored on site, or within sixty (60) days if stored off site. The regulations also mandate that PHI must be maintained for a minimum of six (6) years. Note that the "more stringent" New Jersey law requires that you keep patient records for a minimum of seven (7) years from the date of the last entry in the record.

Patient Requests to Amend PHI

Patients may request that their PHI be amended. A request to amend may be denied for any of the following reasons: 1) the PHI was not created by the covered entity; 2) the PHI is not part of the record available for inspection; or 3) the record is already accurate and complete. A denial of a request to amend PHI must be provided to the patient in writing, and contain specific information set forth in the privacy regulations. The provider has sixty (60) days from the date of receipt of a request to respond; a one-time only thirty (30) day extension is permitted. If an extension is needed, the provider must notify the patient in writing, stating the reason for the delay, and the date that the response to the request will be provided.

Marketing

- Definition of marketing is “to make a communication about a product or service to encourage recipients of the communication to purchase or use the product or service”
- Exceptions to the definition of “marketing” are communications about: 1) the patient’s treatment; 2) descriptions of networks and covered services provided by a covered entity; and 3) case management or recommendations for treatment alternatives and care options.
- Any communication that meets the definition of marketing and does not qualify as an exception requires an authorization prior to the use of PHI for any marketing-related purpose.
- Healthcare communications such as disease management, wellness programs, prescription refill reminders, and appointment notices are permitted.
- Authorization is required before a covered entity may send a patient any marketing materials, sell a patient mailing list, or disclose a patient’s PHI to another person for marketing purposes.

Medical Research

The Privacy Rule permits covered entities to use and disclose PHI for research purposes where specific conditions are met. The Privacy Rule defines research as “a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.”

A covered entity may use or disclose for research purposes PHI that has been de-identified or its use or disclosure authorized by the individual. The general requirements for authorizations apply, along with several specific authorization provisions for research. A research authorization may also be combined with a consent form to participate in the research or with any other legal permission related to the research.

The Privacy Rule also allows covered entities to use and disclose PHI for research in certain circumstances, without the patient’s authorization:

- Documented Institutional Review Board (“IRB”) or Privacy Board approval based upon meeting specific criteria and requiring documentation of specific information pertaining to the waiver
- Preparatory to Research with use or disclosure only for preparation of a research protocol or similar preparatory purposes
- Research on PHI of Decedents permits use of Limited Data Sets with a requisite Data Use Agreement.

Accounting of research disclosures of PHI is not required for disclosures made with a patient’s authorization or for disclosures of the limited data set to researchers with a data use agreement. A simplified accounting of disclosures with patient authorization is permitted where at least 50 records are involved; in such cases, the accounting consists of a list of all protocols for which the PHI may have been disclosed, along with the researcher’s name and contact information.

Other requirements also apply to clinical research. Consultation with your IRB or a qualified health law attorney is recommended.

Complying with the Privacy Rule

The following outlines the necessary components that your practice must have in place in order to comply with the HIPAA Privacy Rule regulations:

1. Designate a Privacy Officer to perform the following responsibilities:

- Oversee the HIPAA compliance program (may delegate tasks)
- Perform a “gap” assessment to compare where your privacy practices, policies and procedures are, or need to be, in order to be HIPAA compliant
- Develop and implement HIPAA policies and procedures and review and revise as needed
- Document your practice’s efforts to be HIPAA compliant
- Handle patient privacy rights complaints, employee sanctions for HIPAA privacy violations and communications with DHHS
 - Note: Sample privacy officer job descriptions are available at www.ahima.org and other websites.

2. Develop a Notice of Privacy Practices that is:

- Written in plain, easily understandable language
- Given to each patient before or at their initial encounter and anytime thereafter upon request
- Posted in a prominent location in your office, and on your practice’s website
- Compliant with the Privacy Rule regulations that specify content in areas of uses and disclosures; patient’s rights; complaints; and duties of the provider
 - Note: Sample notices are available on the internet as discussed above.

3. Develop an Authorization Form

- Note: Sample authorization forms are available on the internet as discussed above.

4. Develop Policies/Procedures for PHI to address the following:

- “Minimum necessary” uses and disclosures of PHI—identify staff who need routine access to PHI and the type of information they need, e.g., nurse would have access to complete medical record as opposed to a receptionist who may only need access to the information on the face sheet
- Handling requests regarding PHI
- Mechanisms to track and document uses and disclosures of PHI
- Safeguards to protect PHI
- Handling patient complaints re: practice’s HIPAA compliance
- Dealing with privacy policy/procedure infractions by staff

5. Train Staff about the Privacy Rule

- Training required for all staff, based on their job functions, i.e. role-based
- Employee training was required by April 14, 2003. If not done already, provide training *as soon as possible*. New employees must be trained within a reasonable time after they start work
- Training must be documented—dates, attendees and topics
- Varied training formats permitted such as lunch hour discussions, self-teaching videos and printed material
- Additional training required for all employees upon changes to HIPAA regulations or to a practice’s privacy policy/procedures

6. Identify Your Business Associates and Review Existing Contracts

- Business Associates (“BA”) are defined as persons who provide certain functions, activities or services involving the use or disclosure of PHI *on behalf of a covered entity*, e.g., physician’s answering service, collection agency, accountant.
- Covered entities are required to have written contracts with their BAs that contain specific safeguards to prevent misuse of PHI and require the BA to assist them with complying with their HIPAA patient rights obligations.
- Covered entities are not liable for the privacy violations of a BA.
- Contracts with BAs must contain specific elements. Model contract language was published with the March 27, 2002 proposed changes and is available from HHS.

Additional Information

The Privacy Rule addresses many other areas including hybrid entities, limited data sets of PHI, and de-identification of PHI. Physicians are advised to consult an experienced health law attorney for information and advice regarding the regulations that have been discussed in general terms above. Other sources of information include professional associations and the Centers for Medicare and Medicaid Services.

Much HIPAA information is also available on the internet. A list of some HIPAA resource web sites is included on the last page of this document.

Selected HIPAA Resources

Centers for Medicare and Medicaid Services (CMS)

<http://www.cms.hhs.gov/HealthInsReformforConsume/HIPAATitleIBulletins/list.asp>

CMS HIPAA page.

Office of Civil Rights (OCR)

<http://www.hhs.gov/ocr/hipaa>

OCR HIPAA page. Includes December 4, 2002 guidance on the Privacy Rule with explanations of its provisions and FAQ's; September 24, 2003 FAQs on authorizations; and 1/14/05 FAQ's on disclosing PHI in litigation.

American Medical Association (AMA)

<http://www.ama-assn.org/go/hipaa>

AMA web page for HIPAA information and related links.

US Department of Health and Human Services (HHS)

<http://aspe.hhs.gov/admsimp>

HHS HIPAA page

Phoenix Health Systems HIPAA Advisory

<http://www.hipaadvisory.com>

HIPAA news, articles, compliance tips, and ability to view all the HIPAA regulations

HIPAA Pro

<http://www.hipaapro.com/hipaa>

Site for rules, regulations, news, Q& A's, articles and free e-mail newsletter, *HIPAA Weekly Advisor*

The International Association of Privacy Professionals

<http://www.privacyassociation.org>

Site for information on personal data privacy with sample HIPAA privacy officer job description.

This material is not to be construed as establishing professional practice standards or providing legal advice. Compliance with any of the recommendations contained herein in no way guarantees the fulfillment of your obligations as may be required by any local, state or federal laws, regulations or other requirements. Readers are advised to consult a qualified attorney or other professional regarding the information and issues discussed herein, and for advice pertaining to a specific situation.