

# PRIVACY (HIPAA)

## INTRODUCTION

This chapter is intended to be a brief explanation of the HIPAA Privacy Rule, which is a federal law that was developed to help protect your right to privacy and security in connection with the electronic transmission of your health information.

### What is HIPAA?

The Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule) were passed as part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). According to the Privacy Rule, all health care providers and health plans are considered “covered entities” that are required to safeguard your information by complying with the Privacy Rule. These “covered entities,” along with their vendors or “business associates” (defined below) with whom they share health information, must prepare and establish specific policies, procedures and forms for the purpose of ensuring the protection of your health information.<sup>(3)</sup>

Throughout this chapter you will see words identified in quotation marks, which are terms commonly used by the Privacy Rule and require your particular attention.

### What is a covered entity?

A “covered entity” is any entity that is required by law to comply with the Privacy Rule. In general, a “covered entity” includes: (1) health care providers; and (2) and health plans that transmit health information in electronic form.<sup>(4)</sup>

#### *Health Care Provider*

A “health care provider” is a provider of medical or health services and any other person or organization that furnishes, bills, or is paid for health care in the normal course of business. Examples of health care providers include physicians, hospitals, home health agencies and providers of durable medical equipment.

- (3) Examples of “protected health information” include a person’s name, along with all identifiable information about an individual, such as a telephone number, health history, diagnosis, claims history, address, and social security number.
- (4) Along with health care providers and health plans, health care clearinghouses are covered entities. A “health care clearinghouse” includes any public or private entity, including a billing service, repricing company or community health information system that processes or helps to process health information.

***Health Plan***

A “health plan” includes group health plans, health insurance issuers, health maintenance organizations, employee welfare benefits plans, and any other individual or group plan that provides or pays for the cost of medical care. This category will include virtually all group health plans, HMOs, and government health programs (Medicare, CHAMPUS, etc.).

**What is a business associate?**

A “business associate” is a person or entity that arranges, performs, or assists a covered entity in an activity involving the use or disclosure of protected health information. These activities include claims processing, claims administration, data analysis, utilization review, quality assurance, benefit management, and any other similar activity covered by the Privacy Rule.

Examples of business associates are persons providing claims processing, legal services, data aggregation, actuarial services, or other services involving the use of protected health information.

**Why is the covered entity vs. business associate distinction important?**

Covered entities are automatically subject to the HIPAA Privacy Rule. Covered entities are required under HIPAA to sign agreements with their business associates that obligate the business associates to act in accordance with the Privacy Rule to safeguard protected health information. Business associates only become subject to HIPAA when the business associate agreement has been signed and becomes effective.

**What is Protected Health Information?**

“Protected Health Information” or “PHI” is basically individually identifiable health information that either identifies the individual or patient directly or would allow someone to identify the individual or patient indirectly.

Examples of PHI include your name, address, social security number, health history, claims history, information about a doctor’s visit, or information about your health condition.

**What is the Privacy Rule?**

The Privacy Rule is the rule that covered entities and business associates must follow to safeguard and protect your PHI. The general rule is that a covered entity or its business associate may not use or disclose PHI except as otherwise permitted under the law.

**When may PHI be used or disclosed?*****Treatment, Payment, or Health Care Operations***

The Privacy Rule permits PHI to be used or disclosed in several instances. For example, your own PHI may be disclosed to you. Also, your PHI could be disclosed to others pursuant to a valid authorization signed by you.

The Privacy Rule allows covered entities to disclose PHI for purposes of (1) “treatment,” (2) “payment,” or (3) “health care operations.”

***Family Members Exception***

There are certain circumstances in which PHI, without a written authorization from you, may be disclosed to family members or other people as long as you have a right to agree or object before your PHI is disclosed.

***Public Welfare Exceptions***

The Privacy Rule also lists several circumstances, relating to public health or legal/governmental proceedings, in which your PHI may be used or disclosed without your consent or authorization and without giving you an opportunity to agree or object. Most of these circumstances will apply in clinical settings.<sup>(5)</sup>

***De-Identification Exception***

Covered entities may also disclose information that has been de-identified (information from which all identifying characteristics have been removed) in accordance with the Privacy Rule, which provides specific rules regarding de-identifying PHI. PHI may be de-identified by removing information, such as your: name; geographic subdivision smaller than a state, including address, county, and zip code; all elements of dates, including birth date, admission dates, etc.; contact numbers and addresses; social security number; medical record numbers; account numbers; health plan beneficiary numbers; vehicle, device, or biometric identifiers; photographic or other images; or any other unique identifying characteristic. To the extent that health information has been de-identified in accordance with the Privacy Rule, it is not PHI and is not subject to the regulations.

- (5) A covered entity may, to varying degrees, disclose PHI: (1) if required by law; (2) for public health activities; (3) to report abuse, neglect, or domestic violence; (4) for health oversight activities; (5) for judicial and administrative proceedings; (6) for law enforcement purposes; (7) for cadaveric organ, tissue or eye donation; (8) for clinical research purposes; (9) to avoid a serious threat to health or safety; and (10) for specialized government functions. Each of these categories has specific definitions of activities that fit within these categories, and each has limits on the information that may be disclosed.

***Incidental Uses and Disclosures***

An incidental use or disclosure of your PHI is permitted to the extent that it occurs as a by-product of a use or disclosure otherwise allowed under the Privacy Rule. An incidental use or disclosure is permissible only to the extent that a covered entity applies reasonable safeguards as required by the minimum necessary standards explained below.

**What is the “minimum necessary” standard?**

As a general rule, when the covered entity or business associate uses or discloses your PHI, the “minimum necessary” standard applies, meaning that reasonable efforts must be taken to limit the disclosure of your PHI to the minimum information necessary to accomplish the intended purpose of the use or disclosure.

***What is a notice and when is it used?***

The Privacy Rule requires covered entities to give notice to you regarding your rights under the Privacy Rule and the potential uses and disclosures of your PHI. The Privacy Rule contains very specific information about the format of the notice and the information the notice must provide, which include: (1) a specific statement that informs you of the purpose of the notice; (2) a description with at least one example of the types of uses and disclosures the covered entity may make with regard to treatment, payment, or health care operation purposes; (3) a description of the other purposes for which the covered entity may be permitted or required to use or disclose PHI without your authorization; and (4) separate statements required if the covered entity is engaged in certain activities listed in the Privacy Rule.<sup>(6)</sup>

**What is an authorization form and when is it used?**

An authorization allows the covered entity or business associate to use or disclose your PHI to a particular person or entity for a specific purpose. An example of when an authorization may be signed by the patient is when PHI is disclosed for marketing purposes. In general, an authorization permits the disclosure of your PHI to a non-covered entity or a non-business associate, if you decide to sign the authorization.<sup>(7)</sup>

- (6) These activities include, for example, contacting the individual for appointment reminders, sending information about treatment alternatives or other health-related benefits or services and fund-raising activities.
- (7) The Privacy Rule requires that the authorization: (1) describe the information to be used or disclosed in a specific and meaningful way; (2) name or otherwise specifically identify the person or class of persons to whom the disclosure may be made; (3) contains an expiration date or an expiration event that relates to you or the purpose of the use or disclosure; (4) contains statements regarding your right to revoke the authorization in writing, the exceptions to the right to revoke, and a description of how to revoke the authorization; (5) contains a statement that the information disclosed may be subject to disclosure by the recipient and may not be protected by the authorization once in the hands of the recipient; and (6) contains your signature and the date.

**What are the major differences between the notice and authorization?**

The notice is a document that advises you about how the covered entity will use or disclose your PHI and what steps the covered entity will take to protect your PHI. The authorization is a form that you decide whether or not to sign in order for a covered entity to use or disclose your PHI for reasons other than treatment, payment or health care operation purposes.

**What rights do you have with regard to your PHI?**

The Privacy Rule affords you the right to access your PHI, the right to amend your PHI, and the right to an accounting of disclosures of your PHI. These rights are explained in the notice form.

**When is the Privacy Rule effective?**

The Privacy Rule is currently in effect. In general, covered entities must have been in compliance by April 14, 2003. However, small health plans (health plans with annual receipts of \$5 million or less) must have been in compliance by April 14, 2004.

**What happens if a covered entity or its business associate violates the Privacy Rule?**

The Department of Health and Human Services may conduct a compliance review of any covered entity to determine whether that entity is in compliance with the Privacy Rule.

**How does HIPAA interact with state laws?**

The Privacy Rule is a federal law. In general, if there is a conflict between the federal and state law, then the federal Privacy Rule should apply. However, the Privacy Rule also requires that if the laws of a particular state conflict with the Privacy Rule and the state law is more stringent (provides more protections) than the state law, or the portion of the state's law that is more stringent will apply instead of the federal Privacy Rule.