The HIPAA Privacy Rule: How May Covered Entities Use and Disclose Health Information [1]

1. Introduction

This guide covers the ways in which HIPAA-covered entities [2] may use and disclose an individual's health information, and the varying degrees of patient control.

To fully understand this guide, it is important to understand who the Health Insurance Portability and Accountability Act (HIPAA) applies to and what information it covers. HIPAA applies to "covered entities [2]" (health care providers, health plans, and healthcare clearinghouses) and their "business associates [3]." The HIPAA Privacy Rule's protections generally apply to "protected health information [4]" (PHI). For an in-depth discussion of who HIPAA applies to and what information it covers, see Privacy Rights Clearinghouse’s Fact Sheet 8a: HIPAA Basics [5].

2. Medical information uses and disclosures: basics

A covered entity [2] may not use or disclose PHI [6] unless HIPAA allows it or the patient authorizes it in writing. This general rule may sound clear cut, but it is in fact very complex.

a. What is a notice of privacy practices?

Individuals have the right to receive a Notice of Privacy Practices (NPP [7]) describing how a provider or health plan uses and discloses protected health information (PHI).

Patients should receive the NPP on their first visit to a provider, and providers should post the notice where patients may see it in
the office or facility. Health plans such as insurers will typically mail NPPs to patients.

An NPP must:

- describe how the HIPAA Privacy Rule allows the covered entity to use and disclose PHI, and state that it will request the patient's permission for any other reason;
- tell patients about their rights under the HIPAA Privacy Rule;
- tell patients how to file a complaint with the covered entity;
- tell patients how to file a complaint with the HHS Office for Civil Rights (OCR), which is responsible for HIPAA enforcement;
- provide information about a patient's rights to restrict fundraising solicitations; and
- explain the need to obtain a patient's written authorization for marketing or the sale of the patient's PHI.

For more details of what a notice must include, see 45 CFR § 164.520 [8] and the HHS website [9].

HHS/OCR has published a variety of model notices [10] to assist health plans and providers with developing their own notice of privacy practices.

b. What does it mean to "consent" versus to "authorize"?

The HIPAA Privacy Rule uses [11] the terms "consent" and "authorization" (two terms that are easy to confuse) to describe very different degrees of patient control.

"Authorization" is much more formal than "consent" and involves a patient granting signed permission. For example, a covered entity [2] may (but doesn't have to) get patient consent when it uses or discloses protected health information [6] (PHI) for treatment, payment, and health care operations. When it comes to obtaining consent, covered entities have a lot of discretion, and even if the covered entity chooses to obtain consent it may be very informal.

c. What is the “minimum necessary” standard?

HIPAA covered entities [2] must make reasonable efforts to limit their use or disclosure of PHI to the “minimum necessary to accomplish the intended purpose.” It is up to the covered entity rather than patient to determine what “minimum necessary” means. Also, there are some situations to which the minimum necessary standard does not apply. For example, it doesn’t apply to information disclosed in connection with treatment or when a patient authorizes a use or disclosure of information. For more information on the minimum necessary standard, see 45 CFR § 164.502(b) and 45 CFR § 164.514(d) [8].

d. Does the Privacy Rule apply to protected health information after death?

Yes. A covered entity [2] must comply with the general rules concerning the uses and disclosures of protected health information for 50 years after the individual's death. For more information, see 45 CFR § 164.502(f). [8]

3. When may a covered entity use or disclose protected health information without obtaining consent?

a. Treatment, payment, and health care operations.

Under HIPAA, a covered entity [2] may seek consent to carry out treatment, payment, and health care operations [12] (sometimes referred to as TPO). Remember that state law [13] may be stricter (this guide does not discuss state laws).

What are "health care operations"? While "treatment" and "payment" are relatively straightforward terms, "health care operations" is less clear and includes the activities a covered entity [2] engages in to run its business.

Health care operations include activities such as:

- reviewing the competence of health care professionals;
- training programs;
- certification and licensing of health care professionals and institutions;
- business planning and development;
- resolving internal grievances;
- sale, transfer, merger, or consolidation of the health care provider of health plan;
- patient safety activities under the Patient Safety and Quality Improvement Act of 2005 [14]; and
- medical review, legal services, auditing, and fraud detection.

For a complete list of activities included in the definition of "health care operations," see 45 CFR § 164.501 [8].
b. Business associates

A covered entity [2] does not need to obtain consent when it shares health information with a business associate [3]. Business associates provide services to covered entities including: legal, actuarial, debt collection, and financial. A contract [15] called a "business associate agreement" creates a legal relationship between the covered entity and the business associate. The business associate may not use or disclose PHI in any way that would violate its contract or HIPAA.


c. Other uses and disclosures that do not require patient consent

It is almost impossible for a patient to account for every person who may see their medical information. Covered entities [2] may use or make the following disclosures without obtaining a patient's authorization or offering them the ability to agree or object:

- uses and disclosures required by law;
- uses and disclosures for public health reporting, and other public health activities;
- disclosures about victims of abuse, neglect, or domestic violence;
- uses and disclosures for health oversight activities such as audits, investigations, and inspections;
- disclosures for judicial and administrative proceedings [16];
- disclosures for law enforcement purposes;
- uses and disclosures to coroners, medical examiners, and funeral directors;
- uses and disclosures for organ, eye or tissue donation;
- uses and disclosures for research purposes (subject to qualifications and exceptions);
- uses and disclosures to avert a serious threat to health or safety;
- uses and disclosures for specified government functions including: military and veterans activities, national security and intelligence activities, protective services for the President and others, medical suitability determinations, and correctional institutions; and
- disclosures for workers' compensation.

Please note that many of the uses and disclosures listed above have their own rules and conditions. For more information, see 45 CFR § 164.512 [8].

In addition, covered entities may use or disclose a limited data set (protected health information (PHI) that excludes certain identifiers) for research, public health, or health care operations purposes without obtaining consent. However, it must obtain a data use agreement from the recipient of the data that meets certain standards. For more information, see 45 CFR § 164.514(e) [8].

4. When must a covered entity obtain patient authorization?

In general, a covered entity [2] must obtain authorization to use or disclose protected health information (PHI) unless the Privacy Rule permits or requires the use or disclosure. For example, the Privacy Rule explicitly allows entities to use and disclose PHI for treatment, payment, and health care operations without authorization.

There are three specific situations where a covered entity must obtain written authorization unless of course it falls under an exception or is already a permitted use or disclosure (see 45 CFR § 164.508(a) [8]):

- for the use and disclosure of psychotherapy notes;
- for the use and disclosure of PHI for marketing; and
- for any disclosure of PHI which is a sale.

Substance abuse treatment programs may also be subject to the HIPAA authorization requirement if the program operates as a covered entity. For example, a treatment program would be subject to this requirement if it deals with a health plan by submitting claims, coordinating benefits, or inquiring about an individual's eligibility, coverage, or benefits or claims status.

HIPAA does not address authorization for disclosures of individually identifiable information about HIV or sexually transmitted diseases, but many states have laws that do. To learn more about states' authorization requirements, see George Washington University's Health Information and the Law website [13].

a. What information should an authorization contain?
An authorization must always include:

- a description of the information that the covered entity [2] will use or disclose;
- the person who is authorized to use or disclosure the information;
- the person to whom the covered entity may disclose the information;
- a description of each purpose of the requested use or disclosure;
- an expiration date; and
- the patient’s signature (or a personal representative who has shown his/her authority to act on behalf of the individual) and date. 45 CFR § 164.508(c)(1)(i)-(vi) [8].

HIPAA also requires authorizations to contain certain statements. Among other things, these include an individual’s right to revoke the authorization in writing and the statement that a provider cannot condition treatment on a patient signing an authorization.

To learn more about authorizations [17] under HIPAA, see the HHS website and 45 CFR § 164.508 [18].

b. Marketing and patient authorization

Covered entities [2] must obtain patient authorization before they use or disclose PHI [6] for marketing purposes. Under the Privacy Rule, “marketing [19]” means communicating about a product or service in a way that encourages a recipient to purchase or use the product or service. Whether a communication is “marketing” often depends on whether the covered entity is paid in exchange for encouraging a product or service. If a covered entity is receiving payment to market a product or service, that must be included in the authorization.

i. When is patient authorization unnecessary?

Face-to-face communications. A covered entity [2] does not have to obtain an individual’s authorization for face-to-face communications (even if the communication would otherwise be considered marketing).

Promotional gifts. A covered entity does not have to obtain authorization if it offers a patient a promotional gift of nominal value. For example, a hospital can provide a free package of baby products to a new mother without obtaining authorization.

Refill reminders regarding a patient’s current prescriptions are not considered marketing [20]. However, any payment the covered entity receives to make the communication must be reasonably related to what it costs to make the communication.

Covered entities can make certain communications without patient authorization when they receive no direct or indirect payment for making the communication. For example, a doctor can contact a patient to talk about treatment alternatives, but if a third party pays her to recommend the alternative treatments she must obtain authorization. The ways in which marketers influence providers to use their products and services is a very gray area.

Covered entities don’t have to obtain patient authorization in the following situations as long as the covered entity does not receive payment to make the communication:

- a health care provider communicates to a patient regarding treatment, including: case management; care coordination; and to recommend alternative treatments, therapies, providers, or settings of care;
- a covered entity (typically a health plan) communicates with an individual to describe a product or service that it provides or includes in its benefits plan; or
- a covered entity communicates information about treatment alternatives for case management or care coordination activities that do not fall under the definition of “treatment.”

To learn more about marketing and how the rule is applied in certain situations, visit the HHS website under the heading “Marketing [21]” or read 45 CFR § 164.501 and 164.508(a)(3) [8].

c. When can a covered entity sell protected health information?

A covered entity [2] must get patient authorization to sell an individual’s protected health information (PHI). In addition, the authorization must state that the covered entity is receiving payment.

A sale of PHI occurs when a covered entity or business associate receives direct or indirect payment in exchange for PHI. A sale does not necessarily mean that there is a transfer of ownership. For example, a covered entity must obtain authorization to receive payment to disclose information, to provide access to information, or to license or lease information. In addition, a health plan (such as an insurer) would have to obtain authorization before it could sell a list of its customers to a drug
company that wants to target market its product.

The following examples are not "sales," and a covered entity does not have to get a patient’s written authorization when it:

- discloses PHI for public health purposes;
- discloses PHI for some research purposes where the only payment is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI;
- discloses PHI for treatment and payment purposes;
- sells, transfers, merges or consolidates all or part of the covered entity;
- provides an individual access to his or her own records;
- pays a business associate for its services; and
- discloses PHI for a purpose that HHS deems necessary.

**Tip:** Individuals should read any authorization they are asked to sign, ask questions, and refuse to sign an authorization unless they are comfortable.

For more information see 45 CFR § 164.502(a)(ii); 164.508(a)(4) [8].

5. When does a covered entity need to provide individuals with an opportunity to agree or object to a use or disclosure?

   a. Hospital directories

Under the Privacy Rule, patients can determine whether they want their information disclosed in a hospital or facility directory.

**What is the purpose of a directory?** A directory allows family members, friends, members of the clergy, and anyone who asks for the individual by name to find a patient. If a patient is not in the directory, the facility will not be able to tell visitors that he or she is there, route calls, deliver flowers, and so on. In emergency situations, a hospital may also receive media inquiries about a patient's condition.

**What information does a directory contain?** A directory typically contains a patient's name and location within the facility. Although there shouldn't be any specific medical data, a directory may contain general information about a person's condition. Directories may also note a patient's religious affiliation, but this should not be revealed to anyone but clergy.

**When may a patient choose whether to disclose information in a directory?** This is typically part of the admission process. At that time, a patient may agree, disagree, or specify that information be shared only with certain individuals.

The health care provider may obtain a patient’s consent or denial verbally. However, if a patient wants to prohibit certain people from having access to directory information, it is always a good idea for the patient to put this in writing.

In an emergency or another scenario where a patient is unable to give verbal consent, a health care provider may use his or her judgment. The provider should then consult the patient when he or she can make an informed choice.

For more information, see 45 CFR § 164.510(a) [8] and HHS’ information about hospital directories [22].

   b. Sharing PHI with family members, friends and others

**When may a covered entity use or disclose a patient’s PHI with another person?**

Generally speaking, covered entities [2] may disclose PHI [4] to anyone a patient wants. They may also use or disclose PHI to notify a family member, personal representative, or someone responsible for the patient’s care of the patient’s location, general condition, or death.

If a patient is present and capable of making a decision, a covered entity should obtain the patient's agreement, provide the patient with the opportunity to object, or use his or her professional judgment to determine that the individual does not object.

If a patient is incapable of making a decision or isn't present, covered entities may use their professional judgment to decide whether a disclosure is in the patient’s best interest.

If the patient is deceased, the provider may disclose protected health information to the people who were involved in the patient’s care or payment prior to death. The only exception to this is when the provider knows that disclosing the information violates a preference that the patient previously expressed.
How much health information may a covered entity disclose? When a covered entity discloses information to another person, HIPAA states that the information should be relevant to that person's involvement in the patient's health care. For example, if a patient is incapable of agreeing, a provider might discuss payment for the treatment with another person directly involved in paying for the care.

The U.S. Department of Health and Human Services (HHS) offers [23] the following examples:

- A doctor may give information about a patient’s mobility limitations to a friend driving the patient home from the hospital.
- A hospital may discuss a patient’s payment options with an adult child.
- A doctor may instruct a patient’s roommate about proper medicine dosage when she comes to pick up her friend from the hospital.
- A physician may discuss a patient’s treatment with the patient in the presence of a friend when the patient brings the friend to a medical appointment and asks if the friend can come into the treatment room.

For more information, see A Health Care Provider's Guide to Communicating with Family, Friends, and Others Involved in the Patient's Care [24] or the HIPAA Privacy Rule at 45 CFR § 510 [25].

6. When may a covered entity use or disclose PHI for fundraising purposes?


A covered entity can use or disclose:

- demographic information including name, address, other contact information, age, gender, and date of birth;
- dates of health care provided to the individual;
- department of service information (e.g. cardiology);
- treating physician;
- outcome information; and
- health insurance status.

a. Can an individual opt out of receiving fundraising communications?

Yes. Each time it makes a fundraising communication, a covered entity [2] must provide a "clear and conspicuous“ opportunity to opt out of receiving further communications. However, individuals should pay attention to the scope of the opt out each time they receive one. A covered entity can exercise discretion over whether to apply an opt out to a specific campaign or to all fundraising in general. Opt outs may not be too burdensome on the individual or cost more than a nominal amount of money.

A covered entity's notice of privacy practices must also state that it may contact the individual to raise funds for the covered entity but that the individual has a right to opt out of receiving the communications. 45 CFR § 164.514(f) [25]

7. How does the HIPAA Privacy Rule apply to uses and disclosures of genetic information?

The Privacy Rule prohibits most health insurers from using or disclosing genetic information for underwriting purposes (such as determining eligibility or setting the cost of premiums). This prohibition applies to group health plans [2] (such as employer sponsored plans), health insurance issuers (including HMOs), and issuers of Medicare supplemental policies. It does not apply to long-term care insurers.

Genetic information includes:

- an individual's genetic tests;
- an individual's family members' genetic tests;
- the manifestation of a disease or disorder in an individual's family members; or
- any request for or receipt of genetic services, or participation in clinical research which includes genetic services, by an individual and his or her family members.

For more information and the precise definition of genetic information, see 45 CFR §160.103 [8] and the HHS website [26]. The World Privacy Forum also has genetic privacy resources [27].