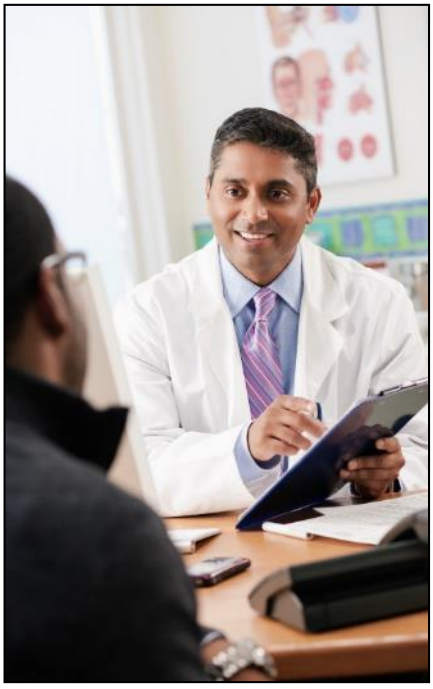
Chapter 3
Understanding Patients' Health Information Rights

Patients' Rights and Your Responsibilities



The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule standards address the use and disclosure of individuals' Protected Health Information (PHI) by organizations subject to the Privacy Rule. The Rule also addresses standards for individuals' privacy rights so that patients can understand and control how their health information is used and disclosed. The Office for Civil Rights (OCR) explains these rights and other requirements more fully on its website, including in its Summary of the HIPAA Privacy Rule,[40] its Frequently Asked Questions (FAQs),[41] and its Understanding Health Information Privacy page.[42]

As a health care provider, you have responsibilities to patients under the HIPAA Privacy Rule, including providing them with a Notice of Privacy Practices (NPP) and responding to their requests for access, amendments, accounting of disclosures, restrictions on uses and disclosures of their health information, and confidential communications.

The Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs (also known as "Meaningful Use" Programs) add new rights for patients who want their health care providers to transmit their electronic PHI (ePHI) to themselves or other caregivers.

Notice of Privacy Practices (NPP)

If you are a Covered Entity (CE), you must provide your patients with a notice of your privacy practices. Your notice must contain certain elements, including:

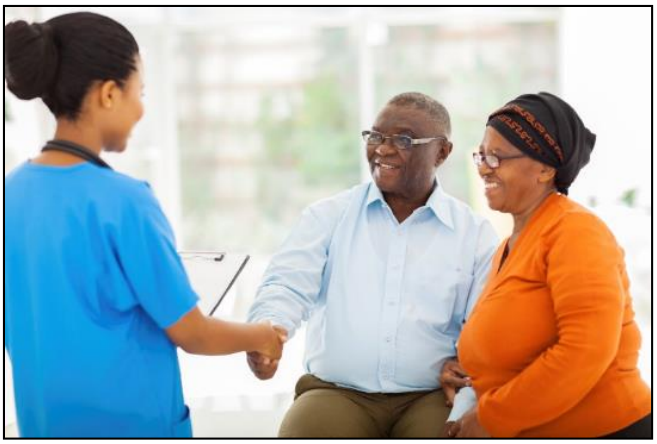
- Description of how your practice may use or disclose (share) an individual's PHI
- Specification of individuals' rights, including the right to complain to the U.S. Department of Health and Human Services (HHS) and to your practice if they believe their privacy rights have been violated (many of these rights are described below)

[40] http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
[41] http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html
[42] http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

- Details of your practice's duties to protect privacy, provide an NPP, and abide by the terms of the notice (OCR provides extensive information for providers, including customizable model notices, on its website. Visit http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/notice.html for requirements and http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html for model notices.)

Patient Access to Information

Patients have the right to inspect and receive a copy of their PHI in a *designated record set*, which includes information about them in your medical and billing records. (Designated record sets are explained at the end of this chapter.) Generally, a CE must grant or deny the request for access within 30 days of receipt of the request. If the health information is held in electronic format and the patient requests to receive it in a specific electronic format, a CE must provide it in the electronic format requested by the patient if it is readily producible. If the format is not available, the CE must provide the health information in an electronic format agreed to by the patient and CE.



Under the Meaningful Use requirements, additional rights apply as well. For example, as your practice gains the capability to demonstrate Stage 2 Meaningful Use, you will be required to respond to any requests from your patients to transmit an electronic copy of PHI directly to persons or entities they designate. An individual may request that you transmit PHI in your records to his or her Personal Health Record (PHR) or to another physician. Your EHR developers, as your BAs, must cooperate in this obligation.

Amending Patient Information

Under the HIPAA Rules, patients have the right to request that your practice amend their PHI in a designated record set. Generally, a CE must honor the request unless it has determined that the information is accurate and complete. The CE must act on an individual's request for an amendment no later than 60 days after the receipt of the request. If you accept an amendment request, your practice must make the appropriate amendment by identifying the records in the designated record set that are affected by the amendment and providing a link to the location of the amendment. If you refuse the request, additional requirements, including the patient's right to file a statement of disagreement that stays with the health record, apply.

Accounting of Disclosures

Individuals have a right to receive an accounting of disclosures[43] of their PHI made by your practice to a person or organization outside of your practice. An accounting of disclosures is a listing of the:

- Names of the person or entity to whom the PHI was disclosed
- Date on which the PHI was disclosed
- Description of the PHI disclosed
- Purpose of the disclosure

This right to an accounting is limited, as the Rule does not require you to include disclosures made for treatment, payment, heath care operations, and several other purposes and situations.

Your practice is required to provide an accounting of disclosures for the six years prior to the date on which the accounting was requested.

Rights to Restrict Information

Individuals have the right to request that your practice restrict certain:

- Uses and disclosures of PHI for treatment, payment, and health care operations
- Disclosures to persons involved in the individual's health care or payment for health care
- Disclosures to notify family members or others about the individual's general condition, location, or death

If your patient (or another person on behalf of the individual) has fully paid out-of-pocket for a service or item and also requests that the PHI not be disclosed to his/her health plan, your practice cannot disclose the PHI to a health plan for payment or health care operations.[44] You should implement policies and procedures that ensure this directive can be carried out.

Right to Confidential Communications

Your practice must accommodate reasonable requests by your patients to receive communications from you by the means or at the locations they specify. For example, they may request that appointment reminders be left on their work voicemail rather than home phone voicemail.

[43] OCR has issued a Notice of Proposed Rulemaking (NPRM) proposing changes to the right to accounting provisions in the Privacy Rule pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act. Learn more at http://blog.cms.gov/2015/01/29/cms-intends-to-modify-requirements-for-meaningful-use/.

[44] 45 Code of Federal Regulations (CFR) 164.522(a)(1)(vi).

Designated Record Set

Given that the HIPAA rights of access and amendment are specific to a CE's designated record set, review your practice's policy about your designated record set to confirm that the policy specifies that EHRs are a component of the set.

A designated record set is a group of records that your practice or your Business Associate (BA) (if applicable) maintains to make decisions about individuals. For health care providers, the designated record set includes (but is not limited to) a patient's medical records and billing records. CEs are responsible for determining what records should be included as part of the designated record set.

For more information about designated record sets, review OCR's guidance on the HIPAA Privacy Rule's Right of Access and Health Information Technology.[45]

[45] http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/eaccess.pdf