



Know Your Benefits

HIPAA Basics

Your right to privacy

Federal regulations place restrictions on how personally identifiable health information may be used and disclosed by certain organizations. These regulations (the Privacy Rules) implement the privacy requirements contained within the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

While some states have laws that protect health information, the HIPAA Privacy Rules establish a uniform, minimum level of privacy protections for all health information.

In summary, the HIPAA Privacy Rules:

- Set limits on how health information may be used and disclosed;
- Require that individuals be told how their health information will be used and disclosed;
- Provide individuals with a right to access, amend or copy their medical records;
- Give individuals a right to receive an accounting of disclosures, to request special restrictions and to receive confidential communications; and
- Impose fines where the requirements contained within the regulations are not met.

Restrictions on Use & Disclosure

The rules allow health care providers, health plans, and health care clearinghouses (Covered Entities) to use and disclose your personally identifiable health information for purposes of treatment, payment or health care operations.

For example, your health care provider may submit your health information to a health insurance company in order to seek payment for the treatment provided to you. Your primary care physician can share your health information with a specialist that he or she recommends you consult. In these cases, your written permission to disclose your health information is not required.

In general, any use or disclosure not considered treatment, payment or a health care operation requires your written authorization, unless an exception applies. For example, your physician may not share your health information with your employer or a life insurance carrier without your written permission.

However, disclosure of health information is permitted for certain purposes specifically listed in the HIPAA Privacy Rules, such as national security, law enforcement and public health issues. If you authorize release of your health information to a third party, the information released may no longer be protected by HIPAA.

Notice of Privacy Practices

You are entitled to receive an explanation of how your personally identifiable health information will be used and disclosed.

For example, a physician or hospital is required to provide you with a Notice of Privacy Practices at your first visit. You will be required to sign an acknowledgement indicating that you received the Notice of Privacy Practices.

If you have health insurance coverage, the insurance company or health plan will also provide you with a Notice of Privacy Practices immediately after you are enrolled in the plan. It is important that you read the Notice of Privacy Practices in order to understand your rights and know who to contact if you feel your privacy rights have been violated.



Know Your Benefits

Right to Access, Amend or Copy

You have a right to view and copy your medical records. You may be charged a fee for the cost of reproduction. If you believe that information within your medical records is incorrect or if important information is missing, you have a right to request that your medical records be amended.

Right to an Accounting of Disclosures

You also have a right to a list of uses and disclosures made of your medical records where the use or disclosure was not for purposes of treatment, payment, health care operations, or pursuant to your written authorization.

Right to Request Restrictions

You may request in writing that a health care provider or health plan not use or disclose information for treatment, payment, or other administrative purposes unless specifically authorized by you, when required by law, or in emergency circumstances. Health care providers and health plans must consider your request, but are not legally obligated to agree to those restrictions.

Also, you can ask your health care provider not to tell your health insurance company about care you receive or drugs you take, if you pay for the care or drugs in full and the provider does not need to get paid by your insurance company.

Right to Confidential Communications

You have a right to receive confidential communications containing your health information. Health care providers and health plans are required to accommodate your reasonable requests. For example, you may ask that a physician contact you at your place of employment or send communications regarding treatment to an alternate address.

Violations of Privacy Rights

If you believe that your privacy rights have been violated, you may contact the Privacy Officer for the organization that you feel has violated your right to privacy. The name of the Privacy Officer should be included in the Notice of Privacy Practices provided to you by that organization.

If the Privacy Officer does not adequately resolve your concerns, you may contact the Department of Health and Human Services — Office of Civil Rights (OCR). OCR is responsible for enforcing the HIPAA Privacy Rules. Its website contains instructions on how to file a complaint www.hhs.gov/ocr/privacy/hipaa/complaints and a complaint form www.hhs.gov/ocr/privacy/hipaa/complaints/hipcomplaintpackage.pdf.

Penalties for Noncompliance

The HIPAA Privacy Rules do not provide individuals with a private right to sue, although individuals may be able to use their HIPAA rights as the basis for claims under other laws, such as ERISA.

Currently, health care providers, health plans, and health care clearinghouses that do not comply with the HIPAA Privacy Rules may be subject to civil money penalties ranging from \$100 to \$50,000 per violation, with maximum penalties ranging from \$25,000 to \$1.5 million per year.

Criminal violations of the HIPAA Privacy Rules may also be referred to the Department of Justice for enforcement. Criminal penalties for such violations include:

- \$50,000 and/or up to one year in prison for knowingly obtaining or disclosing protected health information not permitted by law;
- \$100,000 and/or up to five years in prison for obtaining or disclosing protected health information under false pretenses; and
- \$250,000 and/or up to ten years in prison for obtaining protected health information with an intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm.

State Attorneys General (AG) may also bring suit against Covered Entities to enjoin further violations and obtain damages on behalf of residents of their states, if HHS has not already taken action. The AG may seek damages of up to \$100 per violation, with a maximum of \$25,000 per year for identical violations.



Know Your Benefits

More Information

To learn more about your health information privacy rights, visit www.hhs.gov/ocr/privacy.