



Protecting Your Privacy and Security

Protecting the Privacy and Security of Your Health Information

Federal laws require that health insurers and most health care providers that handle your health information (also known as covered entities) have policies, practices and safeguards in place protecting that information. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security and Breach Notification Rules are the primary Federal laws requiring such protections for your health information.

- [The HIPAA Privacy Rule](#) outlines the rights you have over your own health information, whether it is in electronic or paper format, held by covered entities and sets limits on how your information can be used and shared.
- [The HIPAA Security Rule](#) requires that administrative, technical and physical safeguards are in place to keep your health information secure when it is in an electronic format.
- [The Breach Notification Rule](#) requires that you are notified if your health information, whether electronic or on paper, held by a covered entity or their business associates is seen by or made accessible to someone who is not authorized to see it. This requirement helps patients know if something has gone wrong with the protection of their information.

Who Must Follow These Rules

Most health care providers (such as doctors and hospitals) and health insurers must follow these rules. Other entities or organizations covered by these rules include health care clearinghouses that process health information into and out of standard format. It is important to remember that not everyone is covered by these rules. For example life insurers, employers and many schools do not have to follow these rules.

What Information Is Protected

The health information protected by these rules includes any information held by a covered entity that relates to your health, or to the healthcare you have received, and that could be used to identify you. Thus most of your health information is protected by these rules, for example:

- Information your doctors, nurses, and other health care providers put in your medical record.
- Conversations your doctor has about your care or treatment with nurses and others.
- Information about you in your health insurer's computer system.
- Billing information about you at your clinic.

Other Laws

You may have additional protections and health information rights under your State's laws. There are also Federal laws that protect specific types of health information, such as [information related to Federally funded alcohol and substance abuse treatment](#).

Your Privacy Rights

You have important privacy rights under the HIPAA Privacy Rule, including:

- The right to see and get a copy of your health records, and to ask for corrections if the information is wrong
- The right to get a report on when and why your health information was used
- The right to ask to be reached somewhere other than at home, for example if being contacted at home would put you in danger
- The right to ask that your information NOT be shared

The HIPAA Privacy Rule allows certain health care providers and health insurers to use and share your information without your permission for such key purposes as treatment, payment and health care operations. However, for many other purposes, for example sales calls or advertising, your authorization is required.

If you think your rights are being denied, or your health information isn't being protected, you have the right to file a complaint with your provider or health insurer. The privacy notice you receive from your provider or health insurer will tell you who to contact and how to file a complaint. You can also [file a complaint with the Office for Civil Rights](#).

Safeguards to Protect Your Health Information

The Security Rule requires that your electronic health information is kept secure with administrative, technical, and physical safeguards. These safeguards are designed to make sure that only the right people have access to your information.

The healthcare providers and healthcare insurers that have to follow the law must:

- Put in place safeguards to protect your health information, such as technical safeguards like requiring passwords and encrypting information.
- Have agreements in place with anyone with whom they share health information [also known as a business associate] to make sure that they only use and share your health information according to the law.
- Have procedures in place to limit who can access your health information.
- Train employees about how to protect your health information.

More Information

The Office for Civil Rights of the U.S. Department of Health and Human Services has more information about your privacy rights at: <http://www.hhs.gov/ocr/privacy/>.

Be Responsible

While Federal law can protect your health information, you should also use common sense to make sure that private information doesn't become public. If you access your health records online, make sure you use a strong password and keep it secret. Keep in mind that if you post information online in a public forum, you cannot assume it's private or secure.

