SOURCE: Office for Civil Rights, U.S. Department of Health and Human Services

UPDATED: August 2010

What is HIPAA?

The federal Health Insurance Portability and Accounting Act's Privacy Rule gives you rights over your health information and sets rules and limits on who can look at and receive your health information. The Privacy Rule applies to all forms of individuals' protected health information, whether electronic, written, or oral. The Act's Security Rule, which protects health information in electronic form, requires entities covered by HIPAA to ensure that electronic protected health information is secure.

Who must follow the law?

We call the entities that must follow the HIPAA regulations ***covered entities***.

Covered entities include:

- **Health Plans**, including health insurance companies, HMOs, company health plans, and certain government programs that pay for health care, such as Medicare and Medicaid.
- **Most Health Care Providers**—those that conduct certain business electronically, such as electronically billing your health insurance—including most doctors, clinics, hospitals, psychologists, chiropractors, nursing homes, pharmacies, and dentists.
- **Health Care Clearinghouses**—entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

Who is not required to follow these laws?

Many organizations that have health information about you do not have to follow these laws**.**

Examples of organizations that do not have to follow the Privacy and Security Rules include:

- life insurers,
- employers,
- workers compensation carriers,
- many schools and school districts,
- many state agencies like child protective service agencies,
- many law enforcement agencies,
- many municipal offices.

What information is protected?

- 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
- Most other health information about you held by those who must follow these laws

How is this information protected?

- Covered entities must put in place safeguards to protect your health information.
- Covered entities must reasonably limit uses and disclosures to the minimum necessary to accomplish their intended purpose.
- Covered entities must have contracts in place with their contractors and others ensuring that they use and disclose your health information properly and safeguard it appropriately.
- Covered entities must have procedures in place to limit who can view and access your health information as well as implement training programs for employees about how to protect your health information.

What rights does the privacy rule give me over my health information?

Health insurers and providers who are covered entities must comply with your right to:

- Ask to see and get a copy of your health records
- Have corrections added to your health information
- Receive a notice that tells you how your health information may be used and shared
- Decide if you want to give your permission before your health information can be used or shared for certain purposes, such as for marketing
- Get a report on when and why your health information was shared for certain purposes
- If you believe your rights are being denied or your health information isn't being protected, you can
    - File a complaint with your provider or health insurer
    - File a complaint with the U.S. Government

You should get to know these important rights, which help you protect your health information.

You can ask your provider or health insurer questions about your rights.

Who can look at and receive your health information?

The Privacy Rule sets rules and limits on who can look at and receive your health information

To make sure that your health information is protected in a way that does not interfere with your health care, your information can be used and shared:

- For your treatment and care coordination
- To pay doctors and hospitals for your health care and to help run their businesses
- With your family, relatives, friends, or others you identify who are involved with your health care or your health care bills, unless you object
- To make sure doctors give good care and nursing homes are clean and safe
- To protect the public's health, such as by reporting when the flu is in your area
- To make required reports to the police, such as reporting gunshot wounds

Your health information cannot be used or shared without your written permission unless this law allows it. For example, without your authorization, your provider generally cannot:

- Give your information to your employer
- Use or share your information for marketing or advertising purposes
- Share private notes about your health care

How to report a HIPAA violation

- If you believe that a covered entity violated your (or someone else's) health information privacy rights or committed another violation of the Privacy Rule or Security Rule, you may file a complaint with Office for Civil Rights in the U.S. Department of Health and Human Services. OCR can investigate complaints against covered entities. To file a complaint by e-mail, click on this link:

http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html

SOURCE: Office for Civil Rights, U.S. Department of Health and Human Services

UPDATED: August 2010