From Department of Health and Human Services

HIPAA: WHAT IS IT AND HOW DOES IT WORK?

Most of us believe that our medical and other health information is private and should be protected, and we want to know who has this information. The Privacy Rule, a Federal law, 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 Security Rule is a Federal law that requires security for health information in electronic form.

HIPAA RIGHT OF ACCESS VIDEOS

OCR has teamed up with the HHS Office of the National Coordinator for Health IT to create Your Health Information, Your Rights!" a series of three short, educational videos (in English and option for Spanish captions) to help you understand your right under HIPAA to access and receive a copy of your health information.

Individual's Right under HIPAA to Access their Health Information

HIPAA Access Associated Fees and Timing

HIPAA Access and Third Parties

HIPAA GENERAL FACT SHEETS

Your Health Information Privacy Rights - PDF

Privacy, Security, and Electronic Health Records - PDF

Sharing Health Information with Family Members and Friends - PDF

WHO MUST FOLLOW THESE LAWS?

We call the entities that must follow the HIPAA regulations "covered entities" and they 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.

In addition, business associates of covered entities must follow parts of the HIPAA regulations.

Often, contractors, subcontractors, and other outside persons and companies that are not employees of a covered entity will need to have access to your health information when providing services to the covered entity. We call these entities "business associates." Examples of business associates include:

Companies that help your doctors get paid for providing health care, including billing companies and companies that process your health care claims

Companies that help administer health plans

People like outside lawyers, accountants, and IT specialists

Companies that store or destroy medical records

Covered entities must have contracts in place with their business associates, ensuring that they use and disclose your health information properly and safeguard it appropriately. Business associates must also have similar contracts with subcontractors. Business associates (including subcontractors) must follow the use and disclosure provisions of their contracts and the Privacy Rule, and the safeguard requirements of the Security Rule.

WHO IS NOT REQUIRED TO FOLLOW THESE LAWS?

Many organizations that have health information about you do not have to follow these laws, such as:

Life insurers

Employers

Workers compensation carriers

Most schools and school districts

Many state agencies like child protective service agencies

Most 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 THIS INFORMATION IS PROTECTED

Covered entities must put in place safeguards to protect your health information and ensure they do not use or disclose your health information improperly.

Covered entities must reasonably limit uses and disclosures to the minimum necessary to accomplish their intended purpose.

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.

Business associates also must put in place safeguards to protect your health information and ensure they do not use or disclose your health information improperly.