Health Insurance Portability and Accountability Act (HIPAA) Compliance

Return to Governance and Regulation

Health Insurance Portability and Accountability Act (HIPAA) is United States legislation providing data privacy and security provisions for safeguarding medical information that is collected and controlled by Health Plans, Health Care Providers and Health Care Clearinghouses. The law ganed in importance in recent years beause cyber attacks have allowed the medical records data secuirty perimeters to be breached.

The federal law was signed by President Bill Clinton on Aug. 21, 1996. HIPAA overrides state laws regarding the safety of medical information, unless the state law is considered more stringent than HIPAA. https://searchhealthit.techtarget.com/definition/HIPAA

Who Must Follow These Laws?

Return to Top

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.

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?

Return to Top

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
- Most schools and school districts
- Many state agencies like child protective service agencies
- Most law enforcement agencies
- Many municipal offices

What Information Is Protected?

Return to Top

- 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?

Return to Top

- 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.

What Rights Does the Privacy Rule Give Me over My Health Information?

Return to Top

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 HHS

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.

Learn more about your health information privacy rights - PDF.

Who Can Look at and Receive Your Health Information?

Return to Top

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 or sell your information