

HIPAA-Covered Entities and Ways to Submit a Complaint for a HIPAA Privacy Breach

Below is an outline of which types of organizations or individuals are and are not HIPAA-covered entities. Also provided is a brief description of the responsibilities of the Office for Civil Rights (OCR) and the Federal Trade Commission (FTC) and how to submit a complaint to both the OCR and FTC.

The Health Insurance Portability and Accountability Act (HIPAA) was enacted and sets forth a comprehensive set of standards for protecting sensitive patient health information. The HIPAA applies to all entities that fall within the definition of a “Covered Entity”. If “Covered Entity” engages a “Business Associate” to help carry out its healthcare activities and functions, it is subject to HIPAA Act.

If an organization or individual does not meet the definition of a “Covered Entity” or “Business Associate” it doesn’t have to comply with the HIPAA standards. The definitions for both terms are represented in the table below:

Covered Entity	Business Associate	Entity NOT Subject to HIPAA
A health plan, healthcare provider who transmits any health information	A person or entity performs certain functions that involve protected health information on behalf of, or provides services to, a covered entity	A person or entity is not handling Protected Health Information per HIPAA guidelines and Rules
Health Care Providers such as: • <i>Doctors</i> • <i>Clinics</i> • <i>Psychologists</i> • <i>Chiropractors</i> • <i>Nursing Homes</i> • <i>Pharmacies</i>	Third-party administrator that assists a health plan with claims processing Consultant that performs utilization reviews for a hospital	Employers (in their capacity as employers) Life insurance companies Workers' compensation carriers Auto insurance companies (when not providing health benefits)
Health Plans such as: Health insurance companies HMOs Company health plans Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans’ health care programs	Health care clearinghouse that translates a claim from a nonstandard format into a standard transaction on behalf of a health care provider	Schools and school districts (when not providing healthcare services) Law enforcement agencies State agencies not involved in healthcare administration or services

Covered Entity (continued)	Business Associate	Entity NOT Subject to HIPAA
Entities that process nonstandard health information they receive from another entity into a standard one (i.e., standard electronic format or data content), or vice versa.	Independent medical transcriptionist that provides transcription services to a physician	Attorneys (when not working on behalf of a covered entity) Cosmetic service providers (when not processing healthcare transactions) Alternative medicine practitioners (when not processing healthcare transactions) Pharmacies selling over-the-counter products without PHI
		Family and friends of the patient (unless acting as a personal representative) Fitness and health clubs Marketing companies (when not working on behalf of a covered entity) Researchers (when not obtaining PHI from a covered entity)

The **Office for Civil Rights (OCR)** have the oversight responsibilities to:

- Enforce HIPAA Privacy and Security Rule
- Investigate Complaints filed
- Conduct compliance reviews
- Perform trainings that educate and foster compliance
- Impose civil money penalties

If you would like to file a complaint to OCR, you can visit their website at [OCR online portal](#).

The **Federal Trade Commission (FTC)** have the oversight responsibilities to:

- Enforce Privacy and Security rule per FTC ACT
- Investigate Complaints filed
- Impose civil penalty per violation

If you would like to file a complaint to FTC, visit their website at [ReportFraud.ftc.gov](#) or call the toll-free number 1-877-FTC-HELP (1-877-382-4357; TTY: 1-866-653-4261).

While you have the ability to access your health records using your computer, tablet, and/or smart phone, there are ways you can do to keep your information safe.

Protecting Your Private Information:

- Never give out your personal information online or over the phone unless you have verified the person or organization's identity
- Always Research the facts before agreeing to anything
- Never share passwords or Credentials
- Do not write sensitive information (like passwords) on paper or notepad that can easily be seen or is accessible to others
- Use unique usernames and create strong passwords
- Set up Multi-Factor Authentication (MFA) to keep your accounts secure
- Secure paper files shared with healthcare providers

Create and Maintain Strong Passwords

- Have your passwords be at least 8 characters long
- Avoid repetition and common number sequences
- Use capital and lower-case letters as well as numbers and symbols
- Avoid using the same password for different accounts
- Do not send your passwords or private account information over email
- Change your passwords regularly, once a year

Keep Your Computer Secure:

- Update your computer to the manufacturer's current recommendations.
- Run reliable anti-virus software often. Get new versions of the anti-virus software regularly.
- Use reliable anti-spyware tools.
- Don't allow unfamiliar software to be loaded on your computer.
- Use personal firewall software to protect your PC from outsiders getting your information

Be Cautious Using Public Computers

- Be cautious about entering sensitive information or performing transactions on public computers
- If you use public computers, make sure the computer center is reputable
- Check your surroundings, and make sure no one is looking over your shoulder as you enter your passwords or viewing your personal information
- Don't check "remember passwords" on public computers