Overview
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted to protect the security and privacy of personal health data.

HIPAA basics
HIPAA protects the use and disclosure of Protected Health Information (PHI), which includes an individual’s medical information as well as personal identifiers such as name, address, date of birth and Social Security number. PHI is defined as any information in any form or medium that:

› Is created or received by a health care provider, health plan, employer or health care clearinghouse; AND
› Relates to the past, present or future physical or mental health or condition of an individual, or the provision of payment for health care for an individual; AND
› Is individually identifiable.

Under HIPAA, there are three main rules that Covered Entities and Business Associates (defined on next page) must follow.

› **Privacy Rule**, which sets standards for the protection of individually identifiable health information and limits when PHI can be used and disclosed
› **Security Rule**, which outlines safeguards that must be implemented to protect the confidentiality, integrity and availability of electronic PHI (ePHI)
› **Breach Notification Rule**, which requires Covered Entities and Business Associates to provide notice of any privacy “breach”
Who must comply with HIPAA?

Covered Entities and their Business Associates are required to comply with HIPAA rules. Covered Entities are any entities that transmit PHI and ePHI including:

- Health plans (including fully insured and self-funded plans)
- Health care providers who transmit health information electronically (including billing)
- Health care clearinghouses
- Other entities that deal with individually identifiable health information

While the definition of a Covered Entity does not include employer plan sponsors or plans other than health plans, all employers and employees are affected by, and benefit from, HIPAA’s rules.

A Business Associate is any person or organization that performs certain functions for, or provides services to, a Covered Entity that involves access to PHI. These services may include:

- Claims processing and administration
- Data analysis, processing and storage
- Financial or legal services
- Benefits or practice management

If a Covered Entity engages the services of a Business Associate, it must have a written contract or agreement, called a “Business Associate Agreement,” in place. The agreement must detail the permitted uses and disclosures of PHI by the Business Associate and require the Business Associate to protect the PHI. It’s important to note that a broker partner relationship with a Covered Entity would, in most cases, require a Business Associate Agreement be in place due to the nature of information shared.

What is required under HIPAA?

With limited exceptions, HIPAA requires that Covered Entities and Business Associates:

- Use, request and disclose only the minimum amount of PHI necessary
- Implement data security procedures, protocols and policies to protect PHI
- Comply with uniform standards for certain electronic transactions
- Notify individuals if there is a security breach of their PHI

Privacy Rule

A Covered Entity may only use or disclose PHI as HIPAA expressly requires or permits. The Privacy Rule is intended to limit use and disclosure of PHI to the “minimum necessary” and restrict access and use of PHI to identified personnel.

Required and permitted uses of PHI

Required uses and disclosures under HIPAA include:

- Specified activities in compliance with the law such as those involving public health, law enforcement and judicial proceedings;
- Treatment, payment and health care operations;
- When individuals have authorized such disclosure(s) voluntarily or by written and signed consent; and
When the PHI has been de-identified (i.e., enough information has been removed to neither identify nor provide a reasonable basis to identify an individual).  

Even if permitted, a Covered Entity must make reasonable efforts to use, disclose and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure or request.

PHI cannot be used or disclosed for a non-health plan purpose to another plan (such as a pension or disability plan) or for general employment purposes.

Covered Entities may disclose PHI to a Business Associate to allow it to assist the Covered Entity with carrying out functions that are permitted by HIPAA. The Business Associate must provide assurances that it will comply with the Business Associate Agreement in place.

Authorization requirement

Before using or disclosing PHI to third parties for purposes other than what’s permitted under the Privacy Rule, HIPAA requires Covered Entities to obtain an individual’s authorization in writing. The authorization must specify who is authorized to make and receive the disclosures, the specific purpose of the use or disclosure and an expiration date.

Administrative requirements

The Privacy Rule requires a Covered Entity to establish privacy practices and safeguards, designate an employee to act as a Privacy and Security Official, provide HIPAA training to its workforce, and provide a Notice of Privacy Practices.

The Notice of Privacy Practices must provide a clear, easy-to-read explanation of individuals’ rights with respect to their personal health information and the privacy practices that the Covered Entity has in place. The notice should explain how an individual’s PHI is used and protected, as well as what disclosures are prohibited. The U.S. Department of Health & Human Services (HHS) provides model notices and details on notice distribution on its [HIPAA page](https://www.hhs.gov/hipaa/).

Security Rule

The HIPAA Security Rule requires Covered Entities and Business Associates to protect the confidentiality, integrity and availability of ePHI. “Integrity” is defined as ensuring ePHI is authentic and not altered or destroyed in an unauthorized manner. “Availability” means ePHI should be accessible and usable on demand only by an authorized person.

Reasonable and appropriate administrative, technical and physical safeguards must be implemented and maintained to ensure the protection of ePHI against reasonably anticipated security threats and impermissible uses. Required safeguards include securing PHI with password protected systems, limiting physical access to facilities that store ePHI and auditing system access. There are specific standards with which entities must comply; however, the standards are either “required” or “addressable,” which allows Covered Entities to implement solutions that best fit their needs and specific environment.

Breach Notification Rule

HIPAA defines a “breach” as the acquisition, access, use or disclosure of PHI that violates the Privacy Rule or compromises the security or privacy of PHI. There are exclusions to what is considered a breach including: unintentional, good faith acquisition, access or use by an authorized person without further use or disclosure; or a disclosure to an unauthorized person with a good faith belief that the PHI could not have been retained.

---

1. To “de-identify” information in compliance with HIPAA standards, Covered Entities and Business Associates must remove 18 identifiers, including most dates and geographic identifiers, OR have an expert certify that the information is “de-identified.”
Because the primary purpose of HIPAA is to ensure identifiable health information is protected and secured, Covered Entities are required to notify affected individuals, the HHS, and, in some cases, the media of any breach of unsecured PHI. Similarly, Business Associates are required to notify Covered Entities of any breaches at or by the Business Associate. Notification typically must occur within 60 days of the discovery of the breach.

**How is HIPAA enforced?**

The HHS Office for Civil Rights enforces the HIPAA Privacy, Security and Breach Notification Rules. Failure to comply with HIPAA requirements can result in monetary penalties. In some cases, the Department of Justice (DOJ) may also enforce criminal penalties. HIPAA violations may be discovered through claims investigations, anonymous reports or the government may randomly audit a Covered Entity.

Although employers are not Covered Entities, employers are responsible for ensuring that the group health plans they sponsor are compliant with HIPAA. This means that the employees who perform functions on behalf of the health plan or in administration of the health plan need to understand and comply with HIPAA's requirements.

**What can Covered Entities do?**

All Covered Entities, including any health plan sponsored by an employer (whether fully insured or self-insured), should take actions and implement best practices to ensure compliance with HIPAA's Privacy and Security Rules. For employers that sponsor group health plans this includes the following with respect to the plan and any employees that support it.

› Establish policies and procedures to ensure HIPAA compliance – as part of this process, designate a HIPAA privacy officer to be responsible for overseeing the policy and procedures and their implementation.

› Conduct a risk analysis – periodically review policies and procedures to comply with HIPAA and to identify any potential gaps.

› Implement safeguards – put the necessary physical, technical and administrative safeguards in place to protect any PHI that is maintained. Examples include using password protections on electronic devices, restricting and monitoring access to systems containing PHI and storing files and electronic devices in locked cabinets.

› Periodic training – periodically train employees who support the Covered Entity (including an employer-sponsored group health plan) and have access to PHI on the HIPAA policies and procedures as necessary and appropriate to carry out duties and stay current with compliance requirements.

› Document compliance – record the outcome of any risk analysis, how safeguards were established, any HIPAA training provided to the workforce and any other actions taken to comply with HIPAA’s requirements.

The information in this publication is not legal advice or a legal opinion on any specific facts or circumstances. The contents are intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have. Cigna assumes no responsibility for any circumstances arising out of the use, misuse, interpretation, or application of any information supplied in this publication.

All Cigna products and services are provided exclusively by or through operating subsidiaries of Cigna Corporation, including Cigna Health and Life Insurance Company, Connecticut General Life Insurance Company, Cigna Behavioral Health, Inc., and HMO or service company subsidiaries of Cigna Health Corporation. The Cigna name, logo, and other Cigna marks are owned by Cigna Intellectual Property, Inc.