1. Introduction

Nearly everyone recognizes the sensitive nature of health and medical information. However, health information privacy and security are complex topics to navigate for patients and healthcare professionals alike.

The federal regulations that govern health information privacy and security are known as HIPAA, for the Health Insurance Portability and Accountability Act that mandated them. As a patient, it is important to understand HIPAA’s scope and limitations. This guide provides information on HIPAA basics such as who HIPAA applies to and what information it covers.

2. What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that provides baseline privacy and security standards for medical information. The U.S. Department of Health and Human Services (HHS) is the federal agency in charge of creating rules that implement HIPAA and also enforcing HIPAA.

a. A brief history of HIPAA

- 1996 – Congress passed the Health Insurance Portability and Accountability Act (HIPAA).

Most people are familiar with HIPAA as a medical privacy and security law. However, HIPAA’s initial purpose was to set standards for transmitting electronic health data and to allow people to transfer and continue health insurance after they change or lose a job.
In fact, until 2003 there were no national privacy standards for medical information under HIPAA. All protections were based in state law.


  In 2003, HHS [2] issued the first national data privacy and security rules under HIPAA.

  The *Privacy Rule* [3] gives individuals rights with respect to their protected health information (PHI). It also explains how *covered entities* (those who must comply with HIPAA) can use and disclose PHI.


  The *Enforcement Rule* [5] addresses compliance, investigations, and potential penalties for violations of the HIPAA Privacy Rule and Security Rule. The Office for Civil Rights (OCR) within HHS is responsible for enforcing the HIPAA regulations.

- **2009** – The Health Information Technology for Economic and Clinical Health (HITECH) Act was signed into law. The HITECH Act is Title XIII of the American Recovery and Reinvestment Act (AARA).

  Between 2003 and 2009 technology changed the medical privacy landscape. Electronic medical records started replacing paper files. Patients began to communicate with their doctors by email and through online portals. Pharmacies began to process prescriptions electronically.

  The *HITECH Act* [6] created financial incentives for healthcare providers and insurers to continue shifting to electronic medical records, and also addressed privacy and security concerns related to the electronic transmission of health information, including unauthorized access and data breaches.

- **2013** – HHS’ Office for Civil Rights issued the HIPAA Omnibus Rule.

  HHS’ *Omnibus Rule* [7] made several important changes to the HIPAA Privacy, Security, and Enforcement Rules. It implemented many provisions of the *HITECH Act* [8]. It modified and finalized the Breach Notification Rule. It also implemented changes to the HIPAA Privacy Rule required by the *Genetic Information Nondiscrimination Act of 2008* [9] (GINA).

  b. Is HIPAA the only law that applies to health information?

  No. The Health Insurance Portability and Accountability Act (HIPAA) is not the only law that applies to health information.

  There are federal laws that apply to specific types of health information (or records containing health information) such as genetic information [9], health information in school records [10], identifiable information about individuals maintained by the federal government [11], certain alcohol and drug substance abuse records [12], and information relating to medical research [13].

  In addition, states may enact their own laws to protect health information because HIPAA sets a baseline from which states can create stronger laws. For more information on state law, see [HealthInfoLaw.org] (a project of the George Washington University’s Hirsh Health Law and Policy Program).

  3. Who must comply with HIPAA?

  HIPAA does *not* protect all health information. Nor does it apply to every person who may see or use health information. HIPAA only applies to covered entities and their business associates.

  a. Covered entities

  There are three types of *covered entities* [15] under HIPAA.

  - **Health care providers** get paid to provide health care. Doctors, dentists, hospitals, nursing homes, pharmacies, urgent care clinics, and other entities that provide health care in exchange for payment are examples of providers.

    Health care providers must comply with HIPAA only *if they transmit health information electronically in connection with covered transactions*. Most providers transmit information electronically to carry out functions such as processing claims
and receiving payment. Therefore, most providers are covered under HIPAA.

- **Health plans** pay the cost of medical care.

The following are examples of health plans covered under HIPAA: health insurance companies, health maintenance organizations (HMOs), group health plans sponsored by an employer, government-funded health plans such as Medicare and Medicaid, and most other companies or arrangements that pay for health care.

- **Health care clearinghouses** process information so that it can be transmitted in a standard format between covered entities. Clearinghouses often act as a go between for health care providers and health plans which means that they rarely deal directly with patients. For example, a clearinghouse may take information from a doctor and put it into a standard coded format that can be used for insurance purposes.

For more information on whether an entity is covered under HIPAA, HHS provides a helpful [chart](#)[16].

**b. Business associates**

**What is a business associate?** Health care providers, health plans, and health care clearinghouses are just a few of the players in the health care business. Covered entities hire or contract with people and companies to perform numerous services.

A "business associate" creates, receives, maintains, or transmits protected health information (PHI) on behalf of a covered entity or another business associate acting as a subcontractor.

For the definition of a business associate, see [45 CFR § 160.103](#)[17].

**What do business associates do?** Business associates can perform many different services for a covered entity, including (but not limited to):

- legal
- actuarial
- accounting
- consulting
- data aggregation
- management
- administrative accreditation
- processing or administering claims
- data analysis
- data transmission
- utilization review
- quality assurance
- certain patient safety activities
- billing
- benefit management
- practice management
- repricing.

Business associates often perform services that don’t involve patient interaction. However, a common example of a business associate patients may interact with is a company that offers a personal health record (PHR) to individuals [on behalf of covered entities](#).

**What responsibilities do business associates have?** Covered entities must execute written contracts with their business associates to make sure they safeguard PHI according to HIPAA standards. Business associates must do the same with any of their subcontractors who can be considered business associates. The HHS website contains [more information](#)[18] on business associate relationships, and it also provides sample clauses for business associate agreements.

Business associates must comply with the contracts they sign with covered entities. In addition, business associates are directly liable for violations of the HIPAA security rule and many provisions of the HIPAA privacy rule. This means that business associates are subject to most of the same privacy and data security standards that apply to covered entities and may be subject to HHS audits and penalties.

**c. Subcontractors**

A subcontractor that creates, maintains, or transmits protected health information (PHI) on behalf of a business associate has the
same legal responsibilities as a business associate under HIPAA. In other words, privacy- and security-related legal responsibilities flow “downstream” to subcontractors performing work for a business associate.

For example, a hospital's business associate may hire an outside company to shred documents containing PHI or to provide a cloud service to store the data. In both instances, the outside company (subcontractor) would be required to comply with most HIPAA rules as a business associate. It would also be bound by a contract with the business associate rather than the covered entity (or hospital in this example).

d. Hybrid entities

A hybrid entity performs both HIPAA-covered and non-covered functions as part of its business. A large corporation that has a self-insured health plan [19] for its employees may elect to be treated as a hybrid entity. Other examples are a university with a medical center or a grocery store that has a pharmacy.

When an organization elects to be treated as a hybrid entity, only the portion of the company that is a covered entity (called the health care component) is subject to HIPAA. Hybrid entities must ensure that the health care component does not disclose protected health information to another non-covered component of the business. They must also safeguard electronic protected health information.

4. Who isn’t required to comply with HIPAA?

Remember, a lot of companies and people aren’t required to comply with HIPAA, and there are many times when health information may be available to these people and companies. HIPAA only applies to covered entities and their business associates.

Here are just a few examples of those who aren’t covered under HIPAA but may handle health information:

- life and long-term insurance companies
- workers' compensation insurers, administrative agencies, or employers (unless they are otherwise considered covered entities)
- agencies that deliver Social Security and welfare benefits
- automobile insurance plans that include health benefits
- search engines and websites that provide health or medical information and are not operated by a covered entity
- marketers
- gyms and fitness clubs
- direct to consumer (DTC) genetic testing companies
- many mobile applications (apps) used for health and fitness purposes
- those who conduct screenings at pharmacies, shopping centers, health fairs, or other public places for blood pressure, cholesterol, spinal alignment, and other conditions
- certain alternative medicine practitioners
- most schools and school districts
- researchers who obtain health data directly from health care providers
- most law enforcement agencies
- many state agencies, like child protective services
- courts, where health information is material to a case

To learn more about who is (or isn't) covered by HIPAA, see the HHS Guidance Materials for Consumers [20].

5. What information does HIPAA cover?

To determine whether HIPAA protects a certain type of health information, it is easiest to first figure out whether there is a covered entity or business associate who must comply with the law.

Under HIPAA, “health information” is any information (including genetic information) that is created or received by a health care provider, health plan, public health authority, employer, life insurance company, school or university, or health care clearinghouse and relates to

- a person’s past, present, or future physical or mental health or condition;
- treatment provided to a person; or
- past, present, or future payment for healthcare an individual receives.
Health information can exist in any form or medium, including paper, electronic, or oral.

When a covered entity creates or receives health information that identifies -- or can be used to identify-- a person, HIPAA calls it "individually identifiable health information." Individually identifiable health information includes demographic and other information that identifies a person such as name, address, date of birth, and Social Security number.

For precise definitions of any of the terms in this section, see 45 CFR § 160.103 [21].

a. What information does the HIPAA Privacy Rule apply to?

The HIPAA Privacy Rule applies to "protected health information" (PHI) which includes all "individually identifiable health information" that is transmitted or maintained in any format or medium.

This means that conversations between a patient and a doctor have the same privacy protections as handwritten or electronic notes.

To learn more about the HIPAA Privacy Rule, see: The HIPAA Privacy Rule: How may covered entities use and disclose health information? [22]

b. What information does the HIPAA Security Rule apply to?

The HIPAA Security rule requires covered entities to establish data security measures only for PHI that is maintained in electronic format, called "electronic protected health information" (ePHI). The Security Rule does not apply to PHI that is transmitted orally or in writing.

To learn more about the HIPAA Security Rule, see Privacy Rights Clearinghouse Fact Sheet 8d: Protecting Health Information: The HIPAA Security and Breach Notification Rules [23].

6. What information isn’t covered under the HIPAA Privacy Rule?

a. Health information in employment records

HIPAA does not apply to employment records, even when those records include medical information. This includes employment records a covered entity holds in its role as employer. However, if an employee of a healthcare provider becomes a patient of that provider, HIPAA will apply.

To learn more about medical information in the workplace, see the HHS' Employers and Health Information in the Workplace [24].

b. Health information in education records (for the most part)

Health information in education records that are subject to the Family Educational Rights and Privacy Act (FERPA) is not considered protected health information (PHI) under HIPAA. For example, a child's K-12 records containing information about school nurse visits are not subject to HIPAA.

For more information on FERPA as it relates to health information and HIPAA, see: Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records [25] and Student Privacy 101: Health Privacy in Schools –What law applies? [26]

c. Health information regarding a person who has been deceased for over 50 years

Protected health information (PHI) does not include health information about a person who passed away more than 50 years ago.

For more information on the health information of deceased individuals, see the HHS website [27].

d. De-identified data

De-identified data is health information that has had 18 specific identifiers removed and therefore is considered to make the individual who is the subject of the information unidentifiable. This means de-identified data is not protected under the HIPAA Privacy Rules as PHI and covered entities can use and disclose it more widely.

De-identified data is often the subject of debate because of the possibility of re-identifying an individual. Prof. Latanya Sweeney,
has done a significant amount of work in the area of re-identification.

For more information on de-identification, see 45 CFR 164.514 and HHS’ Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the HIPAA Privacy Rule.

7. How does HHS enforce HIPAA?

The HIPAA Enforcement Rule allows the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) to investigate potential HIPAA violations and assess civil monetary penalties (CMP) for violations. State attorneys general also have the authority to enforce the HIPAA rules. Individuals do not have a private right of action under HIPAA and cannot sue for a violation.

OCR starts the enforcement process by opening an investigation of potential HIPAA Privacy or Security Rule violations. OCR responds to individual complaints, but may discover HIPAA violations in other ways as well (such as conducting audits). After the investigation, OCR can resolve an issue by determining there is no violation, entering into a resolution agreement with the responsible party, or finding that the party is in violation and assessing penalties.

To learn more about HIPAA enforcement, see How OCR Enforces the HIPAA Privacy and Security Rules, Enforcement Data, Enforcement Highlights, and HIPAA Enforcement.

a. When will HHS investigate a complaint?

When individuals are aware of a potential HIPAA violation, they can file a complaint with HHS’ Office for Civil Rights (OCR). To be considered for investigation, a complaint must meet the following basic criteria:

- If the complaint concerns a potential Privacy Rule violation, the action must have occurred after April 2003. If the complaint concerns a potential Security Rule violation, the action must have occurred after April 2005.
- An individual must file a complaint against a person, organization or other entity that is subject to HIPAA.
- The complaint must allege something that would violate the HIPAA Rules.
- Individuals must file complaints within 180 days of the time they knew (or should have known) about the potential violation.

If OCR believes the complaint has merit, the agency will contact the person who filed the complaint as well as the covered entity involved to try and reach a mutual resolution. Some matters may be referred to a hearing before an administrative law judge.

b. How does HHS determine a penalty for a violation?

For violations that occurred after 2009, HHS determines penalties for HIPAA violations based on the violator’s culpability. The minimum penalty varies, but the maximum penalty is $1.5 million per year for violations of the same HIPAA provision.

The four-tiered civil penalty structure is as follows:

<table>
<thead>
<tr>
<th>Violation</th>
<th>Penalty (per violation)</th>
<th>Total civil monetary penalties for violating an identical provision within a calendar year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknowing</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable cause</td>
<td>$1,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful neglect—corrected</td>
<td>$10,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful neglect—not corrected</td>
<td>At least $50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
Unknowing means the covered entity did not know of the violation and would not have known through the exercise of reasonable diligence.

Reasonable cause means the covered entity would have known of the violation by exercising reasonable diligence.

Willful neglect-corrected means that the covered entity intentionally violated HIPAA or acted with reckless indifference but corrected the violation within 30 days of discovery.

Willful neglect-uncorrected means that the covered entity intentionally violated HIPAA or acted with reckless indifference but did not correct the violation within 30 days of discovery.

c. If there’s a monetary penalty, will the individual who filed the complaint receive money?

No. Any money from penalties that HHS collects is paid to the U.S. Treasury.

d. Can individuals sue under HIPAA?

No. Individuals do not have the right to sue under HIPAA. However, HIPAA does not prevent states from passing laws that provide enhanced protection. George Washington University has a guide, Health Information and the Law [42], which contains information on state laws.

8. Resources

Federal Law

Health Information Technology for Economic and Clinical Health (HITECH) Act [43], Public Law 111-5, 2009


Federal Regulations

HIPAA Privacy Rule of 2003 [45] and subsequent modifications

HHS Omnibus Rule [7], 78 Federal Register, January 25, 2013

State Laws and Health Privacy

George Washington University, Health Information and the Law [14] [46]

National Association of Insurance Commissioners [47]

Department of Health and Human Services, Office of Civil Rights

Guidance Materials for Consumers [20]

Special Topics in Health Information Privacy [48]

Business Associate Agreements [49]

Authorizations [50]

Covered Entities [51]

Employers and Health Information in the Workplace [24]

Genetic Information

Department of Health and Human Services (GINA information page) [52]
Council for Responsible Genetics [53]

World Privacy Forum (Genetic Privacy page) [54]

Privacy Rights Clearinghouse
PRC Medical Privacy Resources [55].


Links
[22] https://www.privacyrights.org/content/hipaa-privacy-rule-how-may-covered-entities-use-and-disclose-health-information
[33] https://ocrportal.hhs.gov/ocr/cp/complaint_frontpage.jsf
[34] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html
[38] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html