Privacy Basics

Health Insurance Portability and Accountability Act Basics

Privacy Rights Clearinghouse

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 and enforce it.

Sections to Follow

- A Brief History
- Who Must Comply
- Information Covered
- Information Not Covered
- Individuals' Rights
- Enforcement

A Brief History

1996

Congress Passed the Health Insurance Portability and Accountability Act

Though it is widely known as a medical privacy and data security law, HIPAA was passed primarily to improve the health care system's efficiency and effectiveness. It set standards for transmitting electronic health data and allowed people to transfer/continue health insurance after a job change or job loss. Due to the risks posed by electronic data transfer, HIPAA required HHS to create privacy and security rules. Prior to this, privacy protections for medical information were based in state law.

2000 – 2002

HHS Published and Subsequently Modified the HIPAA Privacy Rule

The HIPAA Privacy Rule gives individuals rights regarding their protected health information (PHI) and sets standards governing how covered entities who conduct health care transactions electronically can use and disclose PHI.

2003

HHS Published the HIPAA Security Rule and Most Covered Entities were Required to Start Complying with the HIPAA Privacy Rule

The HIPAA Security Rule sets standards for safeguarding electronic PHI.

2009

The Health Information Technology for Economic and Clinical Health Act was Enacted as Title XIII of the American Recovery and Reinvestment Act

The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted to promote the adoption and meaningful use of health information technology. It 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

The HIPAA Omnibus Rule made several changes to the HIPAA Privacy, Security and Enforcement Rules by

- implementing provisions of the HITECH Act
- modifying and finalizing the Breach Notification Rule
- implementing changes to the HIPAA Privacy Rule required by the Genetic Information Nondiscrimination Act of 2008

Who Must Comply

HIPAA does not protect all health information or apply to every person who may see or use health information.

Covered Entities

There are three types of covered entities under HIPAA.

Health Care Providers

Health care providers (45 CFR § 160.103) get paid to provide health care. They include

- doctors
- dentists
- hospitals
- nursing homes
- pharmacies
- urgent care clinics

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

Health Plans

Health plans (45 CFR § 160.103) pay the cost of medical care. They include

- health insurance companies
- health maintenance organizations (HMOs)
- group health plans sponsored by an employer
- government-funded health plans (Medicare, Medicaid)
- most other companies or arrangements that pay for health care

Health Care Clearinghouses

Health care clearinghouses (45 CFR § 160.103) 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.

Business Associates

Health care providers, health plans and health care clearinghouses routinely hire or contract with people and companies to perform services. A *business associate* (45 CFR § 160.103) creates, receives, maintains or transmits PHI on behalf of a covered entity or another business associate acting as a subcontractor.

Services

Business associates can perform many different services. Business associates often perform services that don't involve patient interaction including

- legal
- actuarial
- accounting
- consulting
- data aggregation

However, a common example of a business associate with whom patients may interact is a company that offers a personal health record to individuals on behalf of a covered entity.

Responsibilities

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 their business associates.

* The HHS website contains more information on business associate relationships and also provides sample language for business associate agreements.

Business associates must comply with their contractual obligations to covered entities. In addition, business associates are directly liable for violations of the HIPAA Security Rule and many provisions of the HIPAA Privacy Rule—meaning that they 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.

Subcontractors and Hybrid Entities

Subcontractor

A *subcontractor* (45 CFR § 160.103) that creates, maintains or transmits PHI on behalf of a business associate has the same legal responsibilities as a business associate under HIPAA—meaning 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. The outside company (subcontractor) would be required to comply with most HIPAA rules as a business associate and would also be bound by a contract with the business associate rather than the covered entity (hospital).

Hybrid Entity

A *hybrid entity* (45 CFR § 164.103) performs both HIPAA-covered and non-covered functions as part of its business. A few examples are

- a large corporation that has a self-insured health plan for its employees
- a university with a medical center
- 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 and must also safeguard electronic protected health information.

Information Covered

The HIPAA Privacy Rule applies to PHI, and the HIPAA Security Rule applies to electronic PHI.

Health Information

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
- health care clearinghouse

and relates to

- a person's past, present or future physical or mental health or condition
- treatment provided to a person
- past, present, or future payment for healthcare an individual receives.

Health information can exist in any form or medium including paper, electronic or oral.

Individually Identifiable Health Information

Individually identifiable health information identifies—or can be used to identify—a person. It includes demographic and other information that identifies a person such as

- name
- address
- date of birth
- Social Security number

Protected Health Information

Protected health information is individually identifiable health information that is held or transmitted by a covered entity or its business associate.

Information Not Covered

Health Information in Employment Records

HIPAA does not apply to health information in employment records.

* This includes a covered entity's employment records.

Health Information in Education Records (Mostly)

Health information in education records that are subject to the Family Educational Rights and Privacy Act (FERPA) is not considered PHI under HIPAA.

* For more information on health information in education records, 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* and *Student Privacy 101: Health Privacy in Schools—What Law Applies?*

Health Information Regarding a Person Who Has Been Deceased for More Than 50 Years

* For more information on the health information of deceased individuals, see the HHS website's resource.

De-Identified Health Information

De-identified health information has either had 18 types of identifiers removed or been the subject of an expert determination that there is a very small risk that information could identify an individual. De-identified data is often the subject of debate because of the possibility of re-identifying an individual.

* 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*.

Individuals' Rights

Under HIPAA, individuals have the right to

- receive a notice of privacy practices
- see and receive a copy of their medical records
- request that inaccurate information in their medical records be corrected
- request special privacy protections for medical information
- learn who has seen and received their medical information

Enforcement

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 for violations. State attorneys general also have authority to enforce the HIPAA rules. While individuals do not have a private right of action under HIPAA, it does not preempt stronger state laws.

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 (i.e. conducting audits).

1. Individuals can file a complaint with OCR. To be considered for investigation, a complaint must meet the following basic criteria.
2. If the complaint concerns a potential Privacy Rule violation, the action must have occurred after April 2003.
3. If the complaint concerns a potential Security Rule violation, the action must have occurred after April 2005.
4. An individual must file a complaint against a person, organization or other entity that is subject to HIPAA.
5. The complaint must allege something that would violate the HIPAA Rules.
6. 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.

After an investigation, OCR can resolve an issue by

- determining there is no violation
- entering into a resolution agreement with the responsible party
- finding that the party is in violation and assessing penalties

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

Violation	Penalty (per Violation)	Total Civil Monetary Penalties for Violating an Identical Provision Within a Calendar Year
Unknowing[1]	$100 – $50,000	$1,500,000
Reasonable Cause[2]	$1,000 – $50,000	$1,500,000
Willful Neglect—Corrected[3]	$10,000 – $50,000	$1,500,000
Willful Neglect—Not Corrected[4]	At least $50,000	$1,500,000

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

1 The covered entity did not know of the violation and would not have known through the exercise of reasonable diligence.

2 The covered entity would have known of the violation by exercising reasonable diligence.

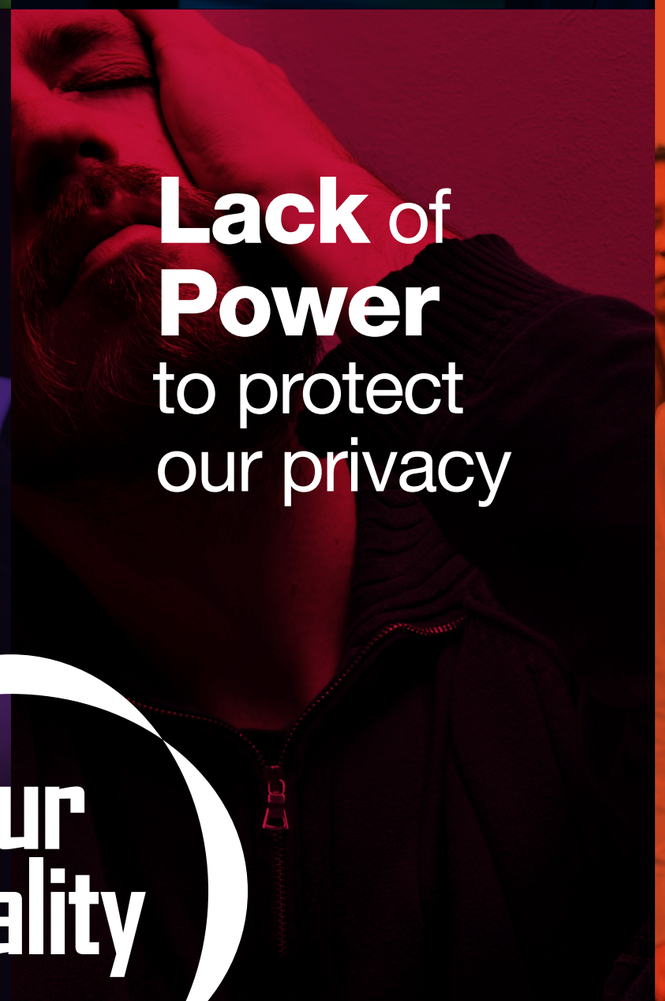
3 The covered entity intentionally violated HIPAA or acted with reckless indifference but corrected the violation within 30 days of discovery.

4 The covered entity intentionally violated HIPAA or acted with reckless indifference but did not correct the violation within 30 days of discovery.

Millions Impacted by **Data Breaches**

No Comprehensive **Right** to **Privacy**

Little Trust in those who **collect**, **use** and **share** our data



Lack of **Power** to protect our privacy

Our Reality

Protecting Privacy for All

Since 1992, Privacy Rights Clearinghouse has been **protecting privacy for all** by **empowering individuals** and **advocating for positive change**.

We hope that this resource has been useful. If you would like to support the development and creation of further educational materials, please consider donating to our organization.

privacyrights.org/donate

Our Mission

Privacy Rights Clearinghouse

3033 5th Avenue
Suite 223
San Diego, CA 92103

O: (619) 298-3396
F : (619) 255-4719

privacyrights.org