What is the Health Insurance Portability and Accountability Act (HIPAA)?

HIPAA, otherwise known as the Health insurance portability and accountability Act of 1996 is a United States law that outlines security and data privacy provisions to keep medical information safe.

The law has become more prominent in the recent past as a result of health data breaches caused by cyberattacks and ransomware attacks on healthcare providers and insurance companies.

President Bill Clinton signed the bill into law on August 21, 1996. As a federal law, HIPAA overrides state laws regarding the safety of medical information unless the state law is more strict than the federal regulation.

What is HIPAA's Purpose?

Also known as public law 104-191, HIPAA has two purposes. One is to provide continuous healthcare coverage for workers who change their job or lose it.

The other is to reduce the cost of healthcare by standardizing electronic

transmission of both administrative and financial transactions.

Additional goals of the law include combating fraud and waste along with abuse in the health insurance and healthcare delivery, while also improving access to long-term care services and health insurance.

The Five Main Parts of HIPAA

The entire law contains five parts, which we outline below.

Title I: Health Insurance Reform

This section of the law protects health insurance coverage for people who lose or change jobs. It also prevents group health plans from denying coverage to people with certain diseases or pre-existing conditions.

It also prevents them from setting a lifetime coverage limit.

Title II: Administrative Simplification

This title directs the US Department of Health and Human Services to establish national standards to process electronic Healthcare transactions.

It also requires health care providers and organizations to implement secure electronic Access to Health Data while also remaining in compliance with any privacy regulations set by the Department of Health and Human Services.

It’s because of this title that we now have the ability to access our healthcare records online and send messages directly to our doctors.

Title III: Tax-Related Health Provisions

In this section, you’ll find the tax-related provisions and guidelines for medical care.

Title IV: Application and Encouragement of

Group Plan Requirements

This area of the law further defines health insurance reform. There are Provisions for individuals with pre-existing conditions and those trying to obtain continued coverage.

Title V: Revenue Offsets

In the final part of the law, you'll find provisions on company-owned life insurance and the treatment of those who lose citizenship for income tax purposes.

HIPAA Compliance Requirements

In the healthcare industry, adherence to Title II is what the majority of people mean when they talk about HIPAA compliance due to how it relates to medical records and other healthcare data.

National Provider Identifier Standard

This requires each Healthcare entity including employers, individuals, health plans, and health care providers to have a unique 10-digit national provider identifier number also known as NPI.

Transactions and Code Sets Standard

This requires healthcare organizations to follow a standardized mechanism for electronic data interchange (EDI) to submit and process insurance claims.

HIPAA Privacy Rule – Standards for Privacy of Individually Identifiable Health Information

This rule establishes national standards designed to protect patient health information. this rule is designed to limit the use and disclosure of sensitive protected health information.

It is designed to protect patient privacy by requiring doctors to provide patients with a list of each entity to which the doctor discloses that information for billing and administrative purposes while still keeping relevant health information

flowing through the proper channels.

The rule also guarantees patients the right to receive their own personal health information upon request from the providers covered by HIPAA.

The privacy rule applies to organizations that are considered covered entities and requires covered entities that work with a HIPAA business associate to produce a contract, or business associate agreement, with specific safeguards on the patient health information that the business associate discloses or uses.

Security Standards for the Protection of Electronic Protected Health Information – HIPAA Security Rule

This part sets the standards for patient data security.

HIPAA Enforcement Rule

This rule creates the guidelines for investigations into compliance violations.

The Department of Health and Human Services Office for Civil Rights (OCR) enforces HIPAA. They perform audits and can issue penalties if they find you in non-compliance. These violations can be quite costly for healthcare organizations.

> *HIPAA compliance is crucial for all covered entities. Failure to maintain compliance can result in costly penalties and potential lawsuits.*

HIPAA-Covered Entities

A covered entity refers to any organization or company that directly handles patients personal health information or personal health records. Covered entities are required to comply with HIPAA and HITECH Act (Health Information Technology for Economic and Clinical Health) Act, which mandates protection for personal health information (PHI) and personal health records (PHR).

Healthcare Providers

This includes doctors, psychologists, dentists, chiropractors, clinics, pharmacies, and nursing homes.

Health Plans

Includes health insurance companies, health maintenance organizations (HMO), company health plans, and government healthcare programs like Medicare and Medicaid, including military healthcare programs.

Healthcare Clearinghouse

A health-care clearinghouse is an entity that processes non-standard health information received from another entity into a standard format or vice versa. Examples of healthcare clearinghouses include Community Health Care Systems and billing services used to manage Health Data.

If you're not sure that you qualify as a HIPAA covered entity, you can use the DHHS online tool to determine if they qualify as a covered entity or a business associate and if they must comply with the regulation or not

Information Protected Under HIPAA

The law protects all individually identifiable health information that is either held or transmitted by a covered entity or a business associate. This information can be held in any form including oral, paper, or digital. The information includes but is not limited to:

- name, address, social security number, birth date, biometric identifiers, and any other personally identifiable information,
- past, present, or future mental health or physical health condition
- the details of any care provided to an individual
- and any information concerning the past, present, or future payment for the care provided to the individual that may identify the patient or the information for which there is a reasonable belief that could be used to identify the patient

It does not include employment records or any data that has been de-identified. For example, PHI includes lab reports or hospital bills because the documents contain identifying information such as the patient's name. Information that is not considered PHI is the blood pressure or heart rate data that has been collected by a consumer health device since it is not shared with a covered entity.

Administrative Requirements

Under the HIPAA law, covered entities must:

- Have a privacy official on staff responsible for developing and implementing policies and procedures.
- Train employees including volunteers on policies and procedures
- Maintain appropriate administrative, physical, and technical safeguards to protect the privacy of personal health information
- Have a process that allows individuals to make complaints about policies and procedures in place.
- Personal health information is disclosed in violation of policy and procedure, the covered entity has to mitigate to the furthest extent possible any harmful effects

Permitted Uses and Disclosures

The privacy rule defines when a covered entity may use or disclose an individual's personal health information.

If the privacy rules specifically permits are required, such as when the covered entity is using the data themselves or transmitting it to another covered entity, it is allowed. If the subject of the information gives written authorization, it is also allowed.

This is why you are asked when you go to the doctor if there is anyone you would like to have medical information shared with such as your spouse or another emergency contact.

Privacy Rule Violation Penalties

Fines vary depending on the extent of the violation. Penalties are broken into four categories:

- Unknowing violations are $100 each, with an annual maximum of $25K for repeats.
- Reasonable cause for violating is $1K with an annual maximum of $100K for repeat violations.
- Willful neglect, with the violation corrected within a given time period, is $10K per violation, with a $250K annual maximum.
- Willful neglect, with the violation not corrected within a given time period, is $50K per violation, with a $1.5M annual maximum.

Covered entities and individuals who intentionally disclose or obtain personal health information in violation of the privacy rule can be fined up to $50,000 and one year in prison. If the rule is violated under false pretenses, the penalties can be increased to $100,000 and up to 10 years in prison.

Security Rule and Examples

The Office of Civil Rights also enforces the security rule which tries to balance patient security with health technology advancement. Under this rule, entities are required to place both electronic and physical safeguards to keep information secure during passage, maintenance, and reception.

Failure to Encrypt Data

The law requires all data to be encrypted however it doesn't specify a specific standard. According to the National Institute of Standards and Technology, Advanced Encryption Standards should be 128 at a minimum.

Failure to encrypt data in storage, devices, and data and Transit could easily constitute a violation.

Unreported Data Breaches

Healthcare organizations are a target for cybercriminals attempting to break into

the network and steal sensitive data.

Covered entities have to report data breaches to the affected individuals along with the Department of Health and Human Services and sometimes the media. This is outlined in the Breach Notification Rule.

One of the easiest ways to avoid a data breach is to ensure that your antivirus software is always current and that data is encrypted throughout storage and transmission.

Keep your software up to date Patch vulnerabilities that hackers used to get into the system. Decommission any outdated devices and remove them from your network. Follow HIPAA regulations to dispose of them properly.

Unauthorized access

Employees accessing data that they don't need or aren't authorized to access, typically constitutes a HIPAA violation.

To avoid this issue, make use of authorization systems that require employees to confirm their identity before accessing restricted information. Establish clear corporate policy and procedure around authorization and consequences for fraudulently accessing information.

Compliance for Employers

The HIPAA Journal has a great checklist for compliance.

- Identify the audits that apply to your organization.
- Conduct internal audits and analyze the results, then determine necessary corrective actions
- Implement and document the corrective measures. Review compliance every year.
- Designate someone to be a HIPAA compliance office or hire dedicated security and privacy offices.
- Have the compliance officers train all the staff on HIPAA obligations
- Document the training and staff member completion of the program.
- Perform due diligence assessments every year on any business associates

to ensure compliance
- Establish processes for reporting breaches and notifying the HHS.

What’s your goal today?

1. Use PLANERGY to manage purchasing and accounts payable

We’ve helped save billions of dollars for our clients through better spend management, process automation in purchasing and finance, and reducing financial risks. To discover how we can help grow your business:

- Read our case studies, client success stories, and testimonials.
- Visit our “Solutions” page to see the areas of your business we can help improve to see if we’re a good fit for each other.
- Learn about us, and our long history of helping companies just like yours.

Book a Live Demo

2. Download our guide “Preparing Your AP Department For The Future”

Download a free copy of our guide to future proofing your accounts payable department. You’ll also be subscribed to our email newsletter and notified about new articles or if have something interesting to share.

download a free copy of our guide

3. Learn best practices for purchasing, finance, and more

Browse hundreds of articles, containing an amazing number of useful tools, techniques, and best practices. Many readers tell us they would have paid consultants for the advice in these articles.

Related Posts