HealthTechWiz

The Complete Developer's Guide To Implementing HIPAA Compliance

A Web Application Developer's Guide!

> Establish defenses in place to shield patient health information. To learn more about healthcare data protection development, read our guide...
>
> BY HEALTHTECHWIZ

Atlanta

7000 Central Parkway,
Suite 220, Atlanta, GA 30328
(678) 648-7722

00 THE HIPAA ESSENTIALS

THE HIPAA ESSENTIALS

The U.S. Government passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996. It puts in place the standard for sensitive patient data protection. Any organization that deals with health information (PHI) must have the physical, network, and process security measures in place.

The HIPAA Compliance Guide and Its Benefits

It is not an easy task to comply with federal regulations around privacy and healthcare data. This comprehensive guide will give the reader impeccable insights into building HIPAA Compliant stuff and the correct steps you'll need to take to ensure you don't end up in violation of the law.

01 CHAPTER

UNDERSTANDING THE NEED FOR HIPPA

Understanding The Need For HIPPA

The Health Insurance Portability and Accountability Act, also referred to as HIPAA, was created to safeguard sensitive health information. According to the law, anyone dealing with sensitive patient data is entitled to protect the privacy and security of preserved health information (PHI). Way back in 1996, HIPAA just served the public with insurance portability.

With portability, privacy concerns started to arise. Thereby the legislators assembled a range of privacy tools and requirements to guard healthcare data. The Four Rules of HIPAA include:

- HIPAA Privacy Rule
- HIPAA Security Rule
- HIPAA Enforcement Rule
- HIPAA Breach Notification Rule

2013 Final Omnibus Rule Update

The U.S. Government passed the Final Omnibus Rule Update in September 2013 that amended HIPAA and considerably answered the definition of who needed to be HIPAA compliant. Earlier, only covered entities such as doctors, hospitals, and insurers were required to be HIPAA compliant. However, with the advent of the 2013 Final Omnibus Rule Update, all entities that store, record, manage or pass PHI are also required to be HIPAA compliant.

The Term That You'll Hear Often

Protected Health Information (PHI)

To put it merely, PHI or Protected Health Information refers to any medical information created, used, or disclosed in providing healthcare services and can potentially identify an individual. PHI can include:

- Health or condition of an individual (Past, Present, & Future)
- Healthcare services rendered to an individual such as
- Billing information from the doctor
- Emails to your doctor's office about a medication
- Emails on prescriptions you need
- Appointment scheduling note
- An MRI scan, Blood test results, Phone records, etc

Covered Entity

Anyone who provides treatment, operations, and payment in healthcare is called a covered entity. According to the U.S. Department of Health & Human Services (HHS), Healthcare Providers, Health Plans, and Healthcare Clearinghouses are all Covered Entities.

Covered Entities are:

- Hospitals
- Doctors
- Clinics
- Psychologists
- Dentists
- Chiropractors
- Nursing homes and pharmacies

Business Associate

A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of or provides services to a covered entity. On the other hand, a member of the covered entity's workforce is not a business associate

02 CHAPTER

THE HIPAA PRIVACY AND HIPAA SECURITY RULES

The HIPAA Privacy And HIPAA Security Rules

According to the U.S. Department of HHS - Health and Human Services, the HIPAA Privacy Rule establishes national standards to protect individual health information. Plus, the Security Rule authorizes a national set of security standards for safeguarding specific health information held or transferred in electronic form.

The Security Rule puts into operation the Privacy Rule's protections by approaching the technical and non-technical safeguards that related entities must operationalize to secure individuals' electronic PHI (e-PHI).

What Is Covered In The HIPAA Security Rules?

- Full names or last name and initial
- All geographical identifiers smaller than a state
- Dates directly related to an individual such as birthday or treatment dates (Other than years)
- Phone Numbers including area code, Fax number/s, Medical record numbers,
- Health insurance beneficiary numbers, Bank Account numbers
- Email address/es, Social Security number
- Certificates/drivers license numbers, Vehicle identifiers
- Device identifiers & serial numbers
- Web Uniform Resource Locators (URLs), Internet Protocol (IP) address numbers
- Biometric identifiers, including fingerprints, retinal, genetic Information, and voiceprints
- Full-face photographs and any comparable images that can identify an individual

What Is Not Covered In The Security Rules?

Information such as:

- Blood sugar reading
- Temperature scan
- Heart rate monitor

In 1996, the law was devised when X-rays were handed out as physical copies, and protecting patient information meant keeping files in locked filing cabinets. A quick forward to the present, it is challenging to determine whether you are using consumer health information or PHI.

A developer creating a health app for a product that transmits health data that can be used to identify an individual personally, then the information is considered PHI, and your organization is subject to HIPAA. If the developer is sharing this data with a covered entity, the developer needs to worry about HIPAA compliance.

03
CHAPTER

HOW TO BECOME HIPAA COMPLIANT?

How To Become HIPAA Compliant?

HIPAA Violations can land in some severe penalties. Besides that, the HIPAA Security Rule wants organizations to take proactive actions against threats to the sanctity of PHI. Therefore Organizations must implement administrative, technical, and physical safeguards to ensure the confidentiality and integrity of the
PHI under their care.

HIPAA Requirements:

HIPAA security law requires the following four things:

- Establish data protection methods for patient health information.
- Limit the use and sharing of data to accomplish the intended purpose.
- Set up Business Associate Agreements (BAAs) and service providers (Business Associates) to adequately use, safeguard, and disclose patient information.
- Methods to restrict who can obtain patient health information and training programs about protecting patient health information.

What it means for developers

Developers who store or transmit PHI to a covered entity should definitely be HIPAA compliant. Stick on to the administrative compliance issues, and there are two ways to approach it on the law's technical and physical aspects.

04 CHAPTER

WHO CERTIFIES HIPAA COMPLIANCE? HIPAA FINES WHO CERTIFIES?

Who Certifies HIPAA Compliance? HIPAA Fines Who Certifies?

No one certifies HIPAA Compliance. However, these are the measures that an organization needs to take to become HIPAA compliant to protect the PHI under an organization's care:

- Organize regular employee HIPAA training and awareness programs to ensure that the staff is aware of cybercriminals' tactics and more mundane and traditional methods of protecting data.
- Buying data loss prevention software such as endpoint security solutions and encryption.
- Policies are in place to prevent employees from accessing PHI via non-secure methods and controlling access to PHI.
- Storing and transmitting PHI via a technique that meets HIPAA compliance - if a third-party provider manages this, then be sure to sign up a business associate agreement to ensure that the third party is also complying with HIPAA.

HIPAA Fines

The HIPAA Compliance fines are expensive to pay. Some of the organizations in the past have paid large sums for being non-compliant. Noncompliance penalties are levied on the negligence level and range from $100 to $50,000 per violation (or per record), with a maximum penalty of $1.5 million per year for violations of an identical provision.

HIPAA Compliance violation and their respective penalty amounts are outlined in the categorized chart below:

Violation Amount Per Violation Violations of an identical provision in a calendar year

Did Not Know	$100-$50,000	$1,500,000
Reasonable Cause	$1000-$50,000	$1,500,000
Wilful Neglect	$10,000-$50,000	

05 CHAPTER

MOBILE APPLICATIONS

Mobile Applications

According to research, there are more than 30,000 health-related applications in AppStores. Undoubtedly, the numbers are a bit intriguing for an industry that, by all accounts, is just starting to get its bearings when it comes to consumer technology. This is not the end of it but a portal to a new beginning, essentially if Apple goes full-on ahead with its rumored Healthbook. The Healthbook is a health-related version of its integrated Passbook application.

PHI in the application

PHI stands for Protected Health Information. PHI is only considered PHI when an individual could be identified from the information. The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights concerning that information.

User communication

HIPAA's objective basis is to safeguard sensitive information, so it is imperative to recognize, analyze, and rethink how you will communicate with subscribers once they are using your app.

Email

It's widely known that the emails are usually not compliant with HIPAA. Most of the emails cannot often encrypt their contents. Therefore sending information that may contain PHI via email is a HIPAA violation. So, when sending emails from the mobile app, ensure you send via a HIPAA compliant email service provider.

Database/API calls

While integrating with a business associate of a covered entity, be sure your app is compliant. Otherwise, these covered entities will not grant your app access to make API or database calls. Neither will you be able to search or read anything within their database.

Push notifications

While applying notifications on the mobile app, it's crucial that you do not include any PHI in any push notifications from your app as they can appear and be publicly visible even when a phone is locked.

06 CHAPTER

WEARABLE APPLICATIONS

Wearable Applications

Wearable technology, also known as "wearables," is a category of electronic devices that can be worn as accessories, such as fitness trackers, smartwatches, heart rate monitors, GPS tracking devices, and much more. For all application developer for wearables who are building something for personalized data transmitted to HIPAA covered entities (PHI) then makes sure it is HIPAA Compliant. Some of the areas you need to double-check are:

- Default displays
- APIs and data sharing
- Medical devices
- Data encryption
- Data synching

07 CHAPTER

ABOUT HEALTHTECHWIZ

HealthTechWiz

ABOUT HEALTHTECHWIZ

At HealthTechWiz, we make HIPAA compliance easier for healthcare applications. HealthTechWiz aims to ensure that doctors, medical institutions, and healthcare providers receive best-in-class and affordable services. With 10+ years of experience, we closely work with local health care providers, healthcare regulatory authorities, and international stakeholders to design a comprehensive and sophisticated range of software and IT solutions for our clients. We handle all of the technical requirements mandated by the HIPAA Security Rule. Typical integration takes days and saves months of dev time.

Atlanta,

7000 Central Parkway, Suite 220,
Atlanta, GA 30328

Phone: (678) 648-7722
Email: contactus@healthtechwiz.com

The information transmitted, including attachments, is intended only for the person(s) or entity to which it is addressed and may contain confidential and/or privileged material. Any review, re-transmission, dissemination or other use of, or taking of any action in reliance upon this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and destroy any copies of this information.

HealthTechWiz