LANGATE

CHECKLIST

HIPAA Compliance Checklist for Software Development 2022

Why HIPAA Exists 04

What is HIPAA? 04

What are the reasons for HIPAA? 04

HIPAA Compliance Checklist for 2022 05

Secure User Authentication 05

Data Access Restriction 06

Backup and Storage Encryption 07

Data Integrity 08

Secure Data Transmission 09

Trusted HIPAA-compliant hosting service providers 09

HIPAA Activity audit 10

What type of software must be compliant with HIPAA? 10

What's the Subject Matter? 11

What's a covered entity? 11

Examples 11

Working with a software development company 12

Conclusion 13

The Healthcare industry doesn't know bad days. The sector has seen constant growth over the past decade, making it such a lucrative space for health-tech businesses and software development companies.

> **However, every health-related application must be HIPAA compliant. This is one of the most important requirements for any Healthcare software product.**
>
> **The Insurance Portability and Accountability Act (HIPAA) defines rules that protect sensitive patient health information (PHI).**

Failure to comply with HIPAA rules could lead to **horrible fines costing your business millions of dollars (up to $1.5 million).** And considering the irrevocable damage to your company's reputation – you're going to be out of business.

As of May 2022, The Organization of CIVIC rights (OCR) has imposed fines on up to 110 cases for the violation of HIPAA rules, resulting in a total of $131 million. **These fines are no joke!**

$131 mln

Fines of May 2022

Want to build software products that are 100% compliant with HIPAA?

Let's show you just how. At Langate, we've developed multiple top-tier applications for the healthcare industry for 8 years today. This article reveals our complete HIPAA compliance checklist for software development in 2022.

This checklist will help you build HIPAA-compliant applications for any use case in healthcare.

Why HIPAA Exists

To build applications that are compliant with HIPAA, you must understand why the act exists in the first place, and what specific software use cases require obligatory compliance with the rules.

What is HIPAA?

> **The Health Insurance Portability and Accountability Act (HIPAA) is a US federal law that was enacted by the US Congress in 1996. The purpose of this law is to protect the privacy of patient health information, and ensure that it is not used or disclosed without authorization.**

What are the reasons for HIPAA?

The main reason for creating HIPAA rules is:

- Protect patient privacy
- Ensure that medical records are not used or disclosed without authorization

In other words, people must be able to trust their doctors and hospitals with their confidential information without worrying about it being misused or stolen by unauthorized parties.

Healthcare is undergoing a rapid digital transformation and so the protection of sensitive electronic patient health information (EPHI) is primordial. HIPAA was created to protect this information. That's why your health-tech business or software company must adhere to HIPAA guidelines when building software products for use in the healthcare sector.

From national pharmacy chains to major medical centers, group health plans, hospital chains, and even small provider offices, no one in healthcare is free from HIPAA rules.

HIPAA Compliance Checklist for 2022

The HIPAA guidelines all circle around two significant rules according to final published reports from the HHS: The data privacy rule and the data security rule. This is the foundation on which the following checklist is built.

1. Secure User Authentication

HIPAA-compliant systems must provide secure user authentication. This goes for all entities using the application: patients, health personnel, etc. Authentication can be achieved using a variety of methods, including:

- **Password-based authentication;**
- **Biometric authentication;**
- **Multi-factor authentication**

Multi-Factor authentication

Multi-Factor authentication is a requirement for HIPAA compliance. It requires two or more forms of identity verification such as passwords + SMS short codes, before granting access to resources or data. The shortcodes add an extra layer of security to your application. This approach provides stronger security than single-factor methods such as passwords or PINs.

Biometric authentication

Biometric technologies can also be incorporated to guarantee compliance. The technology uses unique physical characteristics, such as fingerprints, to verify that the user is who they say they are. Although biometrics provide greater security than passwords alone, they're not perfect and can be compromised if hackers have access to the same databases as you do.

2. Data Access Restriction

Restricting who gets access to what particular data within your application is a crucial part of HIPAA compliance. Access control policies must be put in place to protect against unauthorized access to patient information. These policies should define who can access certain pieces of data and what they can do with it once they have access. For example, only specialist doctors may have access to sensitive health patient info.

This, of course, begins with role definition and standard HIPAA access control mechanisms. Access logs are also required to keep track of who does what, and ensure non-repudiation.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

> The Security Rule also states that information safeguards must be implemented in accordance with the **National Institute of Standards and Technology (NIST)'s Cybersecurity Framework.**

The NIST Cybersecurity Framework provides an excellent guide for determining what measures should be taken when it comes to protecting your organization's data. **According to the framework, your developers must provide:**

Technical controls

Technical controls that prevent or mitigate unauthorized access, use, disclosure, or modification of your information system, by employing hardware, software, or networking devices and protocols that have been tested by NIST under controlled conditions.

Operational controls

Operational controls that manage system functions and limit access to information systems based on user roles.

3. Backup and Storage Encryption

The HIPAA Security Rule requires companies to encrypt all ePHI when it is stored on mobile or desktop devices. This means you must encrypt whatever sensitive information is intended to sit on the user's phone or computer.

The same security rule requires that all ePHI be backed up in accordance with a written contingency plan. However, the rule does not specify exactly how the backups should be encrypted.

The HHS Office for Civil Rights (OCR) has clarified that backup and storage encryption is required for ePHI when it is stored on an application server or shared drive.

One way to evaluate your current environment is to use the HIPAA Security Risk Analysis template (PDF) provided by HHS OCR.

This tool is designed to help you determine where your organization falls on a scale from low risk to high risk, based on 18 data security factors that have been identified as being essential to protecting patient information.

If your organization scores low on this analysis, you may consider implementing an encryption solution that meets the HIPAA Security Rule requirements.

4. Data Integrity

Data integrity is a crucial element of HIPAA compliance.

In fact, it's one of the seven "administrative simplifications" in the HIPAA Privacy Rule, which requires that covered entities implement policies and procedures to ensure the integrity and confidentiality of ePHI and physical PHI.

The data integrity requirement means your app must protect:

- **PHI or ePHI;**
- **Tampering;**
- **Unauthorized access or use;**
- **Accidental or deliberate loss or destruction.**

It also means you have to make sure that any third-party apps you use are secure enough to handle the task.

In order to meet this requirement, you need two things:

Security strategy	A security strategy that will help you protect PHI from unauthorized access or use by unauthorized persons. This means implementing authentication and authorization controls on all applications that process, store or transmit PHI.
Data backup	A data backup plan that ensures your system can recover from hardware failures, software failures, and other malfunctions so that no patient's information is lost.

5. Secure Data Transmission

The HIPAA Security Rule requires covered entities and their business associates to encrypt the PHI they send over the network or store on portable devices. This includes backup media, such as a hard drive or USB flash drive.

The HIPAA Security Rule allows encryption methods that use a passphrase or key file to access the data. The rule also requires creating backup media with encryption turned on by default.

So if for some reason, sensitive patient information has to be transmitted over a network in the course of use of your application, your developers must employ standard encryption mechanisms to keep you on the safe side.

6. Trusted HIPAA-compliant hosting service providers

The hosting service is always part of your infrastructure. So if you did everything right by HIPAA and still worked with a non-compliant hosting service provider, you're unfortunately not on the safe side.

You must do business with a HIPAA-compliant hosting service provider if you want to build applications for healthcare.

A HIPAA-compliant hosting provider will have physical, technical, and administrative safeguards to protect your data from unauthorized access, disclosure, or modification. **The provider should be certified by an accredited certification body (CB)** or be able to demonstrate that their system has been evaluated by an accreditation organization.

Some major HIPAA-compliant hosting and cloud storage service providers include:

Google Cloud

Amazon Web Services

Microsoft Azure

7. HIPAA Activity audit

An activity audit is a record of all actions that take place in your system during a given time period. It can contain different types of activities such as Logins, logout, user actions, system actions, API calls, database queries, etc.

The purpose of an activity audit is typically to provide evidence that actions were performed according to predetermined standards or guidelines. Activity audits are often used in conjunction with other types of audits (e.g., financial audits) but may be conducted separately as well.

HIPAA regulations require that organizations create an Activity Audit Log (AAL) which must contain detailed information about all accesses made by employees who have access rights to electronically protected health information (ePHI) within their organization. This includes both authorized and non-authorized accesses made by employees

What type of software must be compliant with HIPAA?

While HIPAA rules touch every angle of the health sector, **not all health-related apps MUST be HIPAA compliant.** For example, a simple workout app or basic BMI index calculator app which doesn't collect any patient data doesn't require compliance.

HIPAA requires that all software used by a covered entity and its business associates be coded to comply with the HIPAA Security Rule. The HIPAA Security Rule is designed to protect electronic patient information and requires covered entities and their business associates to implement administrative, physical and technical safeguards to ensure confidentiality, integrity, and availability of ePHI.

Whether your application must be HIPAA compliant depends on two things: the subject matter and the covered entity.

What's the Subject Matter?

The subject matter of your software includes any data or information that can be reasonably linked back to an identifiable individual.

This includes any information that is created or received by your company, regardless of how it is stored or maintained.

For example, if you write a program for a hospital that helps them track patient data and provides a user interface so they can manage this data, then this program would be considered subject matter under HIPAA because it contains patient data that could be linked back to an individual.

What's a covered entity?

A "covered entity" under HIPAA is any person who performs certain functions under HIPAA such as conducting healthcare operations or performing healthcare services on behalf of others in order to receive payment for those services from third-party payors; providing health care billing and collection services.

So, if you're a health-tech startup, software development company, or an established brand looking to build an application or extend your existing application to serve a specific purpose in healthcare, review your subject matter and covered entities to see if HIPAA compliance is a must for you.

Examples...

Here's a short list of some of the software types that must be compliant with HIPAA:

- **Healthcare software systems**
- **Medical billing software**
- **Medical record systems**
- **Patient scheduling systems**
- **Healthcare practice management (HR) systems**
- **EHRs (electronic health records)**

Working with a software development company

If you're a business looking to develop applications to serve the health sector, you need to work with developers or a development company that understands HIPAA requirements and other government regulations to the letter.

That's why Langate with its tremendous wealth of experience in the health industry is the right software dev partner for you.

We have sufficient technical and human resources necessary to build 100% HIPAA-compliant software of any kind.

Let's help you develop compliant applications that may save lives through healthcare and save you millions in penalties.

Learn more about Langate.

Phone: 888 LANGATE x 1
Email: info@langate.com
Skype: langate
Web: www.langate.com

Conclusion

The HIPAA guidelines couldn't have come at a better time. More than ever, they help protect sensitive health information in this digital age.

Building software tools that comply with HIPAA rules should be a priority for your business. The OCR has the capacity to impose heavy fines of up to $1.5 million on software that fails to respect HIPAA rules, so there's reason to be careful.

Our above-recommended checklist builds on the two major rules of data privacy and data security to help you build HIPAA-compliant applications.

Use our comprehensive checklist to develop software that can thrive and scale without borders in the rather meticulously strict health sector.