LANGATE

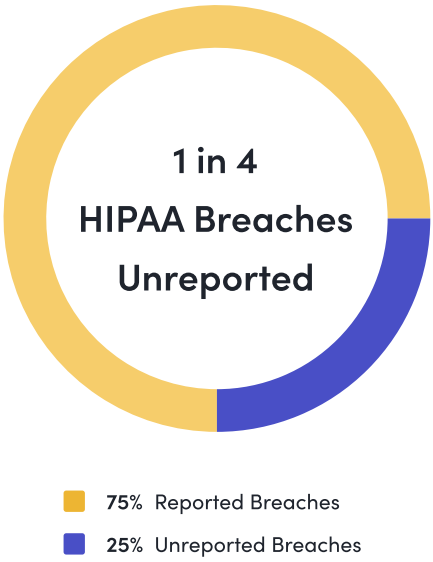
Checklist

HIPAA Compliance Checklist for Software Development 2025

Provided by Langate Software, a HIPAA-compliant development partner trusted by hospitals, SNFs, and other healthcare organizations.

What Is HIPAA?

The healthcare industry has grown continuously over the past decade, making it a lucrative space for health-tech businesses and software development companies. However, at the same time, **healthcare data breaches have been increasing.**



387 Healthcare data breaches

reported to OCR* in Q1 2024

*the Department of Health and Human Services Office for Civil Rights

HIPAA COMPLIANT

All healthcare software products must comply with the **Insurance Portability and Accountability Act (HIPAA)**, which defines rules that safeguard sensitive protected health information (PHI)

DEPARTMENT OF HEALTH & HUMAN SERVICES · USA
Office for Civil Rights

According to final reports from the Department of Health and Human Services (HHS), **HIPAA guidelines revolve around two rules** that form the foundation for the following checklist:

- the HIPAA Privacy Rule
- the HIPAA Security Rule

80% of Healthcare Organizations

fail meaningful use audit

50% of Healthcare Organizations

believe they would fail a HIPAA audit

Failing to comply with HIPAA rules can have serious consequences: severe fines, legal action, and reputational damage. Violations can lose patients' trust and even cause an organization to go out of business.

~ 600 HIPAA Violations

referred to DOJ

1 in 7 Healthcare Organizations

have still not appointed a HIPAA compliance officer

Average cost

per records is $363

Phishing and ransomware

the top hacker tactic

Ransomware

for medical records accelerating rapidly

Unauthorised access for records

accounts for 20% of HIPAA breaches

Taking proactive steps - such as robust access management, regular audits, and thorough employee training - helps mitigate these risks, ensuring both legal adherence and patient data integrity.

~ 200 mln Patient Records

compromised since introduction of HIPAA

$50,000 Severe Fines

for the most serious HIPAA violations, with an annual cap of $1.5 million

Key HIPAA Updates for 2025

The proposed updates to the HIPAA Security Rule in 2025 aim to strengthen standards and implementation specifications by introducing new requirements and clarifying existing ones. **Changes include:**

Strengthening Cybersecurity Measures

The Department of Health and Human Services (HHS) plans to eliminate the distinction between "required" and "addressable" implementation specifications, making all standards mandatory. This change aims to ensure the consistent application of cybersecurity measures across all covered entities and business associates.

Aligning with 42 CFR Part 2

Changes have been made to better align the regulations for the confidentiality of Substance Use Disorder and Mental Health Services Administration patient records with HIPAA standards. This update aims to enhance care coordination and simplify compliance for entities managing both types of sensitive information.

HIPAA and Reproductive Health

The proposed changes aim to revise the conditions under which Protected Health Information (PHI) related to reproductive healthcare can be used or disclosed. These modifications reflect the evolving legal and social considerations regarding reproductive health. The goal is to ensure that healthcare providers can share PHI that aligns with patients' rights and addresses broader healthcare needs.

What Type of Software Must Be HIPAA-Compliant?

HIPAA compliance remains crucial in safeguarding patient data across the healthcare industry, but not all health-related applications need to be compliant. For example, a wellness app that tracks general fitness goals or a basic BMI calculator that does not collect PHI is typically exempt.

HIPAA mandates that any software utilized by a covered entity or its business associates must adhere to the HIPAA Security Rule. This rule, which requires robust administrative, physical, and technical safeguards, ensures the confidentiality, integrity, and availability of electronic protected health information (ePHI).

Ultimately, whether your application needs to be HIPAA-compliant depends on two factors:

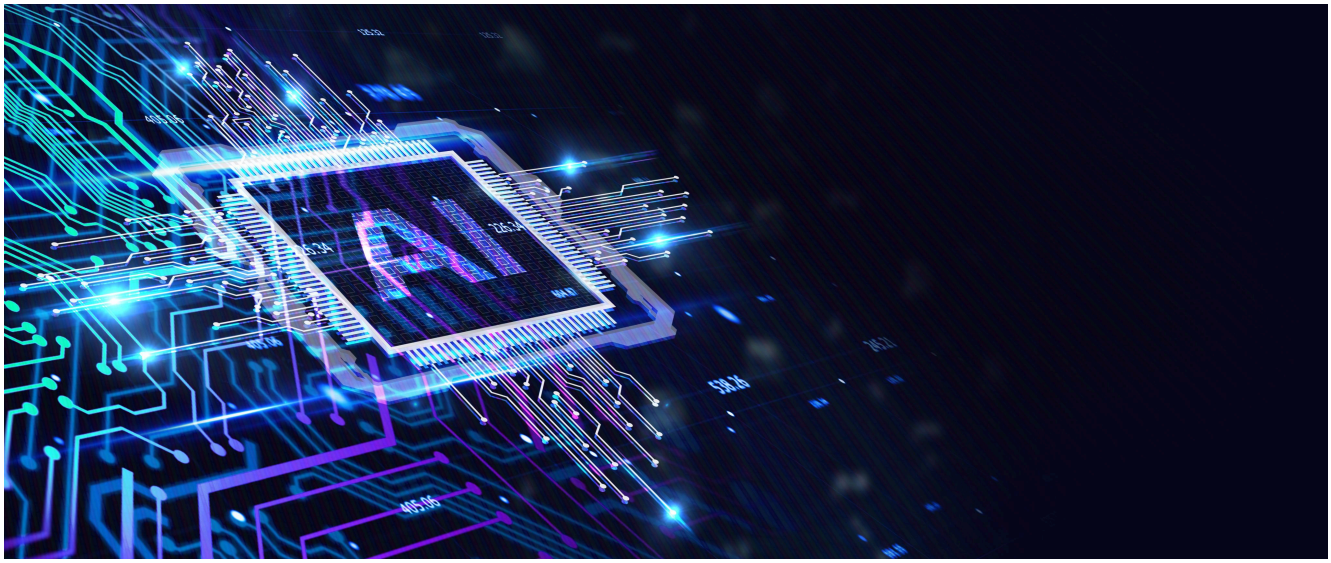
1. The subject matter of the software
2. The involvement of covered entities

What Is the Subject Matter?

The subject matter refers to any data or information within your software that can be reasonably linked back to an individual. For instance:

A program that tracks patient appointments and stores medical records is subject to HIPAA as it contains identifiable health information.

Any software facilitating data entry, processing, or analysis of health data connected to individuals must comply with HIPAA regulations.



> As of 2025, the rise of AI and IoT in healthcare has expanded the scope of "subject matter" to include remote monitoring devices and advanced analytics platforms, making compliance even more critical.

What Is a Covered Entity?

A covered entity is any organization or individual performing functions related to healthcare operations under HIPAA. These include:

Healthcare providers such as hospitals, clinics, and telemedicine platforms

Health plans and insurance companies

Clearinghouses managing health-related billing and claims

Additionally, business associates such as software vendors, cloud storage providers, and IT consultants who handle ePHI are required to comply.

If your business is a health-tech startup or an established provider looking to build or enhance healthcare software, understanding the involvement of covered entities is essential for determining the applicability of HIPAA.

Examples of Software Requiring HIPAA Compliance

As the healthcare industry evolves, the following types of s**oftware often require HIPAA compliance:**

Electronic health record (EHR) and electronic medical record (EMR) systems

AI-powered diagnostics or predictive analytics tools processing patient data

Telemedicine platforms supporting video consultations and ePHI sharing

Remote patient monitoring systems using IoT devices

Healthcare management systems (e.g., patient portals and hospital management platforms)

Medical billing and coding software

Checklist

While various methods exist to evaluate HIPAA compliance, our checklist provides a quick and effective way to assess your operations and identify areas with the highest-risk vulnerabilities; check your box if the answer is yes:

It Is Recommended to Conduct the Following Annual Audits

1. Security risk assessment

- [ ] Identify potential threats and vulnerabilities in your system.
- [ ] Assess the likelihood and impact of security breaches.
- [ ] Evaluate current security measures and controls.
- [ ] Develop a risk management plan to address identified gaps.

2. Privacy standards audit (not required for business associates)

- [ ] Review policies for handling PHI.
- [ ] Assess access controls to ensure only authorized users can view PHI.
- [ ] Verify compliance with patient rights (e.g., access, amendment, disclosures).
- [ ] Check that procedures are in place for responding to privacy incidents and breaches.

3. Security standards audit

- [ ] Ensure encryption is used for data at rest and in transit.
- [ ] Review authentication and access control mechanisms.
- [ ] Assess logging and monitoring of system activity.
- [ ] Verify incident response procedures for security threats.

4. Asset and device audit

- [ ] Maintain an up-to-date inventory of all devices handling PHI.
- [ ] Ensure secure configurations and access controls on all devices.
- [ ] Check for outdated software and apply necessary patches and updates.
- [ ] Enforce policies for lost, stolen, or decommissioned devices.

5. Physical site audit

- [ ] Evaluate physical access controls to sensitive areas (e.g., server rooms).
- [ ] Check security measures such as surveillance, locks, and alarms.
- [ ] Ensure workstations and portable devices are secured when unattended.
- [ ] Review visitor access policies and logging procedures

Maintain HIPAA Privacy Rule Compliance

- [ ] Have you designated a Privacy Officer responsible for developing, implementing, and enforcing HIPAA-compliant policies?
- [ ] Do you have a policy outlining the Privacy Officer's duties, including oversight of privacy practices, handling complaints, and ensuring workforce training? .

Maintain HIPAA Privacy Rule Compliance

- [ ] Do you have a defined process for dealing with incidents or breaches?
- [ ] Do you have the ability to track and manage incident/breach investigations?
- [ ] Can you provide the required reporting of minor or meaningful breaches or incidents?
- [ ] Are staff members able to report an incident anonymously?

You Have to Develop Remediation Plans in Case of Data Breaches

- [ ] Have you created remediation plans to address any deficiencies found in the annual audits?
- [ ] Have you fully documented (in writing) these remediation plans?
- [ ] Do you update and review these remediation plans annually?

Strengthen Your Staff with Proper HIPAA Training and Compliance Oversight

- [ ] Have all staff members received annual HIPAA training?
- [ ] Is staff training documented?
- [ ] Have you designated a staff member as the HIPAA compliance, privacy, and/or security officer?

Ensure Vendor and Business Associate Compliance

- [ ] Have you identified all vendors and business associates?
- [ ] Do you have business associate agreements in place with each of them?
- [ ] Have you performed due diligence on your business associates to assess their HIPAA compliance?
- [ ] Are you tracking and reviewing your business associate agreements annually?
- [ ] Do you have confidentiality agreements in place with non-business associate vendors?

Any unchecked items highlight areas for improvement — addressing them strengthens your compliance posture and helps protect sensitive data. Regularly reviewing your HIPAA compliance helps you stay updated with evolving regulations and ensures data security.

If you want more details download our guide

Conclusion

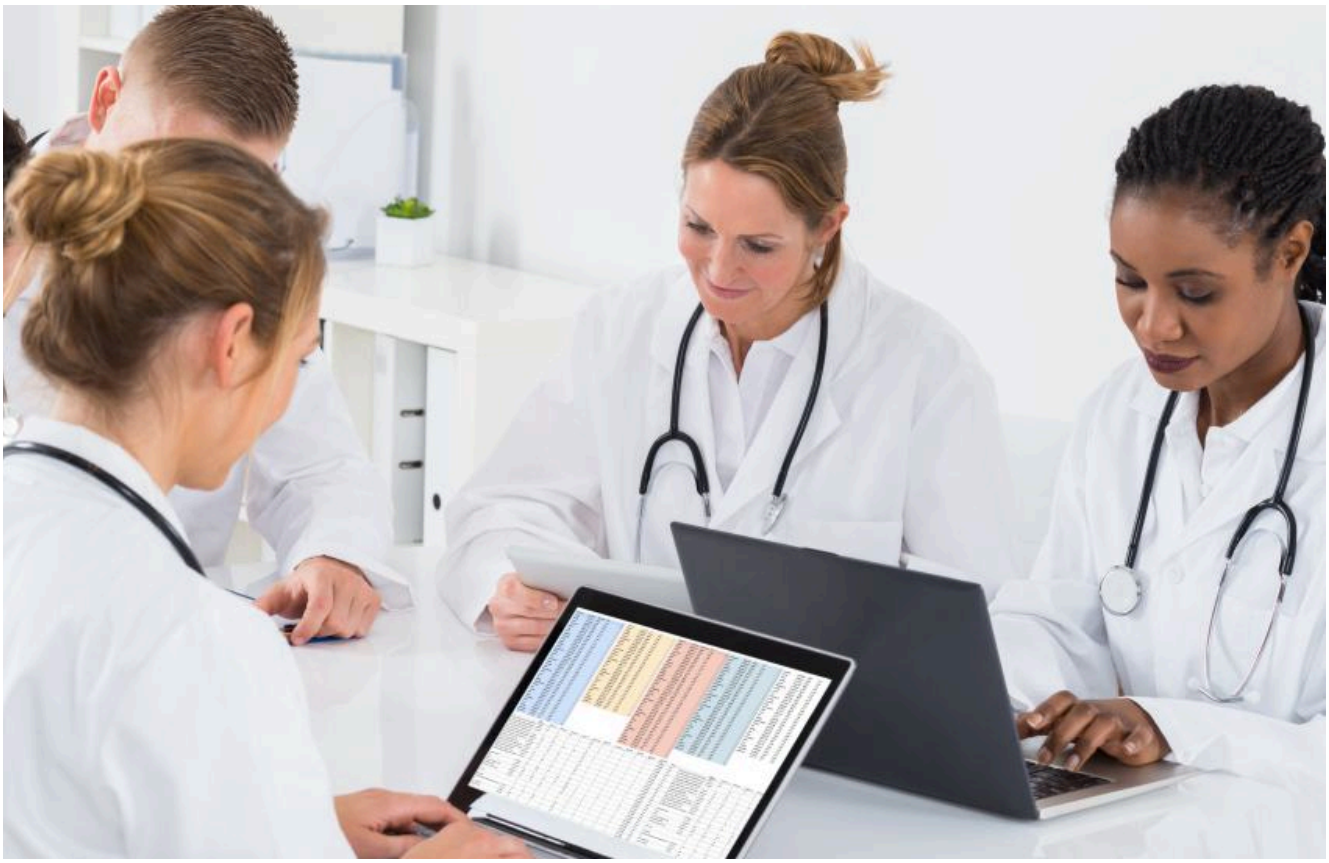
With the healthcare industry increasingly relying on technology, these rules play a critical role in safeguarding sensitive patient data and maintaining trust between providers and patients.

> For businesses developing software in the healthcare sector, HIPAA compliance is not just a regulatory requirement but a vital step toward building secure and scalable solutions. The Office for Civil Rights (OCR) can impose fines of up to $50,000 for the most serious violations (up to $1.5 million per year), so adhering to these standards is of paramount importance.

Following our recommended checklist is a practical way to help your business ensure compliance, protecting it from regulatory risks and reputational damage.

Building HIPAA-Compliant Solutions

If your business aims to develop applications for the health sector, collaborating with developers or a development company that fully understands HIPAA requirements and other government regulations is essential. At Langate, we have the technical and human resources necessary to build 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