Thoropass™

HIPAA requirements for HealthTech SMBs

thoropass.com →

It can be difficult to translate vague, risk-focused HIPAA requirements into actionable controls and policies. What's more, it takes significant time, money, and effort to become HIPAA-compliant.

Yet many HealthTech companies need HIPAA compliance to grow and thrive. Not only do you need to meet HIPAA requirements to handle certain types of data, but they can't even dream of working with customers in the health industry without compliance; federal law (and the customers themselves) simply won't allow it.

To help you start to navigate the complexity of HIPAA compliance, we mapped out the most important things you need to know. This resource explains why HIPAA is important for high-growth businesses, how much it costs, what's involved, and what's recommended for teams of all sizes pursuing compliance.

What Is HIPAA?

Doctors' offices, health insurers, and the tech companies that serve them need to meet federal regulatory compliance rules defined by the Health Insurance Portability and Accountability Act (HIPAA). Among many other things, HIPAA sets national security and privacy standards for certain types of health information and is enforced by the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services.

However, HIPAA was passed in 1996, at a time before smartphones and tech SMBs. It wasn't written with today's health data needs in mind. Since then, lawmakers have updated it several times to better align it with current issues facing the privacy and security of health information.

Does my company need to be HIPAA-compliant?

It depends on the type of business you are. For example, are you a covered entity or a business associate as defined by HIPAA.

Do you handle Protected Health Information (PHI)?

HIPAA Privacy Rule, according to the U.S. Department of Health and Human Services, states that: The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as "protected health information") and applies to health plans, healthcare clearinghouses, and those healthcare providers that conduct certain healthcare transactions electronically.

If your business handles patient records (past or present), payment information, or test results, chances are, you're working with PHI.

On its own, health information (like a blood pressure reading) isn't PHI. Neither is personal information like a name, phone number, or Social Security number. The data is contextual; it depends on where the information came from and how it's being used or who is using it.

PHI can be a combination of health information and any identifier that could link that information to a specific person.

- Health information is data created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school (or university), or healthcare clearinghouse. It includes everything about a person's past, current, and future health (diagnoses, health care coverage, payment for medical services). For example, patient or family medical history records, bills from a primary care physician, or lab results are all considered health information in the eyes of HIPAA.
- Identifiers, on the other hand, include any demographic information that could be used to identify an individual. HIPAA protects 19 identifiers, including names, phone numbers, email addresses, Social Security numbers, account numbers, license plate numbers, photos, fingerprints, genetic information, etc. Identifiers need to be protected only when combined with health information.

Do your customers need you to be HIPAA-compliant?

In many cases, your customers will need your company to comply with HIPAA in order to even consider working with you.

HIPAA applies to two types of organizations: covered entities and business associates.

- Covered entities are health plans, healthcare clearinghouses, or healthcare providers who transmit any health information in electronic form in connection with a transaction.
- Business associates are organizations or individuals who create, receive, maintain, or transmit protected health information on behalf of a covered entity. HR tech companies like WageWorks and Greenhouse may be considered business associates under HIPAA because they handle employee benefits information working with health plans. Something to note is that not all benefits information falls under HIPAA. It depends if they are working with a health plan. In that case, they would sign a BAA with the health plan (covered entity.)

A BAA is a contract that defines how PHI will be used and protected by the business associate. It ensures that the business associate complies with HIPAA and that the covered entity reports and stops working with that vendor if any breaches or violations arise.

But it gets more complicated than that.

Say your SaaS company provides a dashboard that helps healthcare providers manage their PHI. Because you handle PHI for the health care provider, you are a business associate. Data hosting services are considered subcontractors. This is due to the 'persistence of custody' over the PHI the services hold for the business associate. Even if the data was encrypted, the data hosting company is still maintaining custody over the PHI data requiring them to comply with HIPAA.

In this scenario, think of your company as the middle link in a chain of HIPAA compliance. You would need a BAA with the health care provider AND the data host. But the data host wouldn't need a BAA with the health care provider.

What happens if my business isn't HIPAA-compliant?

Usually, an OCR audit doesn't happen unless an employee, customer, or vendor reports your lack of compliance. But if something does happen, then you're subject to some pretty significant fines.

The global average total cost of a data breach from 2020–2022 in the healthcare sector was $10 Million. And in the financial industry, it was 5.97 Million.

It's important to note that actual federal fine amounts depend on the severity of the breach and negligence. The totals also include breach containment and notification costs, business disruption, revenue cost, customer turnover, reputation losses, and other long-term impacts.

As mentioned above, companies in the health industry can't legally work with technology companies without a BAA if PHI is involved. Failing to become HIPAA-compliant means your sales team won't be able to close deals, and your startup will struggle to move upmarket.

What HIPAA requirements do I need to be compliant?

Now that we understand what HIPAA is and why it's important for SMBs, let's look at the HIPAA requirements and frameworks that founders need to know.

How to make sense of HIPAA regulatory requirements

HIPAA is broken up into three different rules: the Security Rule, the Privacy Rule, and the Breach Notification Rule.

The HIPAA Security Rule

The HIPAA Security Rule establishes administrative, physical, and technical safeguards for electronic PHI. It's similar to main security frameworks such as NIST SP 800-53 and ISO 27001.

In adhering to the HIPAA Security Rule, you'll need policies and procedures in place to address the following items, among others:

Administrative

- Risk analysis and management
- Sanctions for employees who don't comply with policies
- Regular review of system activity
- PHI access rights
- Awareness and training (password controls, log-in monitoring, training reminders)
- Incident protocols
- Contingency planning

Physical

- Office/facility access (including contingency access for emergencies)
- Office/facility security
- Device/computer security and access
- Physical PHI storage (device disposal, data backup, etc.)

Technical

- Unique user identification
- Automatic log-off
- Encryption and decryption
- Auditing app and backend activity
- MFA and other authentication
- Integrity controls

For help translating HIPAA's Security Rule requirements for your business, check out these resources:

- Security Risk Assessment Tool: This government-offered application helps small to medium-sized companies navigate HIPAA Security Rule standards.
- NIST HIPAA Security Rule Toolkit: This application helps organizations conduct a self-assessment and identify gaps in Security Rule adherence. (Note: NIST no longer supports this toolkit.)
- Thoropass: We provide custom HIPAA-compliance road maps tailored specifically for your needs. Our team of HIPAA experts will work with you to make compliance quick and pain-free.

The HIPAA Privacy Rule

The HIPAA Privacy Rule sets guidelines for what you can and can't do with PHI. For example, HIPAA's Privacy Rule:

- defines allowed use cases and disclosure of PHI;
- gives individuals access to their PHI, the ability to know who else has seen it, and some control over how their PHI is used;
- makes sure PHI disclosure is limited to only the information that's needed;
- stipulates what organizations have to do in order to protect PHI; and
- establishes penalties for PHI mishandling.

The HIPAA breach notification rule

Once part of the Privacy Rule, the Breach Notification Rule, defines a breach and what must be done if one occurs.

This rule goes into detail about who needs to be notified, how, and when. For example, the rule stipulates that covered entities must, within 60 days of a breach, send first-class mail or an email informing patients whose PHI was put at risk in the breach. It also defines when businesses have to notify the media and the U.S. Department of Health and Human Services.

Choose your HIPAA adventure: Third-party review, HITRUST Certification, or Security Framework

Knowing the three aforementioned rules is just the start. Translating them into actionable objectives takes a bit more work. Thankfully, you have some options to help you with this task.

The OCR provides some resources for organizations to become HIPAA-compliant on their own (see above). However, most companies bring in a third-party reviewer, pursue HITRUST certification, or follow a security framework to make sure they do it right.

Third-party HIPAA Review

A reviewer provides an unbiased report about your policies, procedures, and controls through the lens of HIPAA.

Like other audits (such as a SOC 2 Type 2 audit), an annual HIPAA Compliance Review should require evidence your company actually executes on your policies and validate these controls. It is highly recommended for you to collect evidence to demonstrate your company's compliance with your HIPAA policies/procedures. While there isn't a formal certification for HIPAA, regulators will want to know how effective your controls are, which will then impact their risk analysis requirements.

HITRUST CSF Certification

The Health Information Trust Alliance (HITRUST) is an organization that maintains the HITRUST CSF Common Security Framework, a risk-management framework that pulls from other well-known compliance frameworks (HIPAA, NIST, ISO, PCI).

The HITRUST CSF is more prescriptive than HIPAA while covering the necessary controls.

Security Framework

Many companies pair HIPAA with either the NIST SP 800-53 or the ISO 27001 security framework for additional guidance as they pursue HIPAA's Security Rule.

- **NIST SP 800-53**: This stands for the National Institute of Standards and Technology Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organization. It was published to help federal agencies improve their information security.
- **ISO 27001**: The ISO 27001 framework is a framework for the ISMS (Information Security Management System). ISO 27001 has its own control appendix and is internationally recognized. It's often chosen by growing tech companies that work outside of the United States.

Time and cost of HIPAA compliance

How much time and money should you expect to spend on meeting HIPAA requirements? It depends on a variety of factors.

How long does HIPAA compliance take?

In short, you should expect to spend several months preparing for HIPAA compliance, and anywhere from weeks to months on an actual assessment. However, the exact timeline depends on a number of factors:

- The size and distribution of your organization
- The current lack or abundance of documentation for policies, procedures, and controls
- The complexity and level of risk of data, services, and processes
- The type of compliance verification you choose

For example, if you decide to pursue a HITRUST CSF certification, expect to spend upwards of three to six months in the readiness assessment for an r2 HITRUST Certification, and 90 days on the Validated assessment. You also need to ensure the controls are working for at least 90 days before they can be tested. The length of the engagement depends on the type of assessment you choose to pursue. HITRUST offers a readiness-assessment and a validated assessment by a third-party approved External Assessor, such as Thoropass.

Keep in mind that HIPAA compliance isn't a one-and-done affair. You need to renew your compliance every year. This becomes more important for tech organizations as they mature and their size, services, customers, and complexity increase.

How much does HIPAA compliance cost?

HIPAA compliance costs depend on whether you pursue a third-party assessment or you handle everything in-house.

It's important to note that time and cost often go hand in hand. So it should be unsurprising that your HIPAA compliance cost depends on the same factors that determine how long it will take. Team size, complexity and level of risk, documentation, and type of compliance all come into play here.

According to Security Analyst, Jen Stone (MSCIS, CISSP, QSA), if you are a small covered entity, HIPAA could cost anywhere from $4,000–$12,000 and for medium and large covered entities, anywhere upwards of $50,000, depending on your current environment.

These costs don't include indirect impacts, such as opportunity costs and salary dedication for in-house employees, legal fees, or significant process overhauls and technical needs.

Spend some time window shopping when you're ready to settle on a HIPAA-compliance framework or vendor. Thoropass, for example, helps connect its customers with experienced compliance partners via the Thoropass Partner Ecosystem. You may also be able to save some money by asking your customers if they'll accept a different (less expensive) form of HIPAA validation.

Plus, if you're part of the AWS Marketplace, you can sign up or renew with Thoropass for 5% back. Reach out to a member of our team today to see if you're eligible.

Recommendations for SMBs seeking HIPAA compliance

Although it's not easy to become HIPAA-compliant, we can offer several tactics to make the process less challenging.

Start with risk management, not technical controls

Oftentimes, teams tend to jump straight to technical controls when they start pursuing a new compliance framework. They see the required controls and believe that the best way to start is by getting those in place—not only to make progress but also to protect their data.

Instead, we recommend that you begin building toward meeting HIPAA requirements with a risk-management program. That is because much of HIPAA evaluation is done using a risk-management methodology.

By understanding the possible risks and risk levels before jumping to controls, you better position yourself to identify and implement more appropriate and effective controls. In putting risk management first, you can actually help yourself prioritize and comply faster in the long run.

Limit the PHI you work with

Techniques like data aggregation and tokenization help limit the amount of PHI they need to protect as part of HIPAA compliance.

Data aggregation

Remember that health information is protected by HIPAA only when it's combined with all 19 identifiers that can tie that data back to the corresponding individual. Data aggregation presents health information without the identifiers. Alternatively, you can have an expert perform an analysis to determine and confirm there is no way to re-identify individuals.

For example, a hospital's annual report that provides information about intake numbers, average patient age, and other aggregate data would not be considered PHI because it wouldn't tie any of that health information to the corresponding individuals.

Data tokenization

This technique transforms sensitive information into a senseless combination of characters. It's useful for when you do not need the information (such as PHI or a Social Security number), but you do need to pass this information downstream to a third-party vendor. The PHI then exists within your environment as a token and removes many of the requirements from your systems.

As your company grows, take a hard look at what information you need to collect to serve your customers and what you can leave by the wayside. The less PHI your company needs to handle, the lighter your HIPAA burden.

Build your HIPAA-compliance dream team in-house

In 2021, the United States experienced a shortfall of nearly 314,000 cybersecurity professionals. That shortage is expected to grow to 1.8 million in 2022.

The lack of compliance experts means that people who want to hire them pay more for their expertise and make sacrifices on whom to bring in, or under what circumstances. This reality makes it more attractive to handle HIPAA compliance in-house.

Today, more startups and high-growth SMBs are leaning on compliance solutions like Thoropass to get more breathing room before making a strategic hire or completely replace the need for an external hire.

They're also using a divide-and-conquer approach to handling compliance in-house. That means splitting the responsibility among the team members whose day-to-day jobs already coincide with your security needs. For example, instead of handling HIPAA requirements independently, founders will enlist their engineers to manage HIPAA security controls and assign risk management to an operations team member.

Use a HIPAA-compliance solution like Thoropass

Compliance solutions provide crucial, company-specific guidance for SMBs looking to become HIPAA-compliant.

When leaning on Thoropass as you pursue HIPAA compliance, you'll already know what you need to have in place to meet the expectations of your third-party reviewer. You'll also have time to work on building your risk-management system at your own pace, so you won't have to drop everything when the consultant arrives with their list of controls.

We have in-house expertise for all of your compliance needs (HIPAA, ISO, GDPR, SOC 2, HITRUST, etc.). When you work with Thoropass, you get insight across the board, not just on HIPAA-specific things. You'll have an edge because you'll understand how different compliance frameworks interact to create the best solution for your specific needs.

On a more tactical level, Thoropass makes it much easier to fill out due-diligence questionnaires. Thoropass saves and organizes your responses so you don't have to start from scratch every time. This cuts down that operational burden to under an hour per questionnaire.

Plus, if you use Amazon Cloud Services, like many of our customers, you can easily renew your Thoropass subscription within the AWS Marketplace and earn 5% back. Speak to a member of our team today to see if your organization is eligible!

Compliance is about helping people, not checking off HIPAA requirements

HIPAA's purpose isn't to drive you mad or to drain your org of critical time, money, or energy. HIPAA's goal is to protect people and their important medical information.

When you invest in HIPAA compliance, you're not just opening your startup for business with health providers; you're telling the world that you take the public's privacy, security, and well-being seriously. What's more, HIPAA compliance signals to potential customers that your startup is established and trustworthy, giving you an edge over your competition. It's a solid growth strategy, particularly for startups looking to move upmarket in the health space.