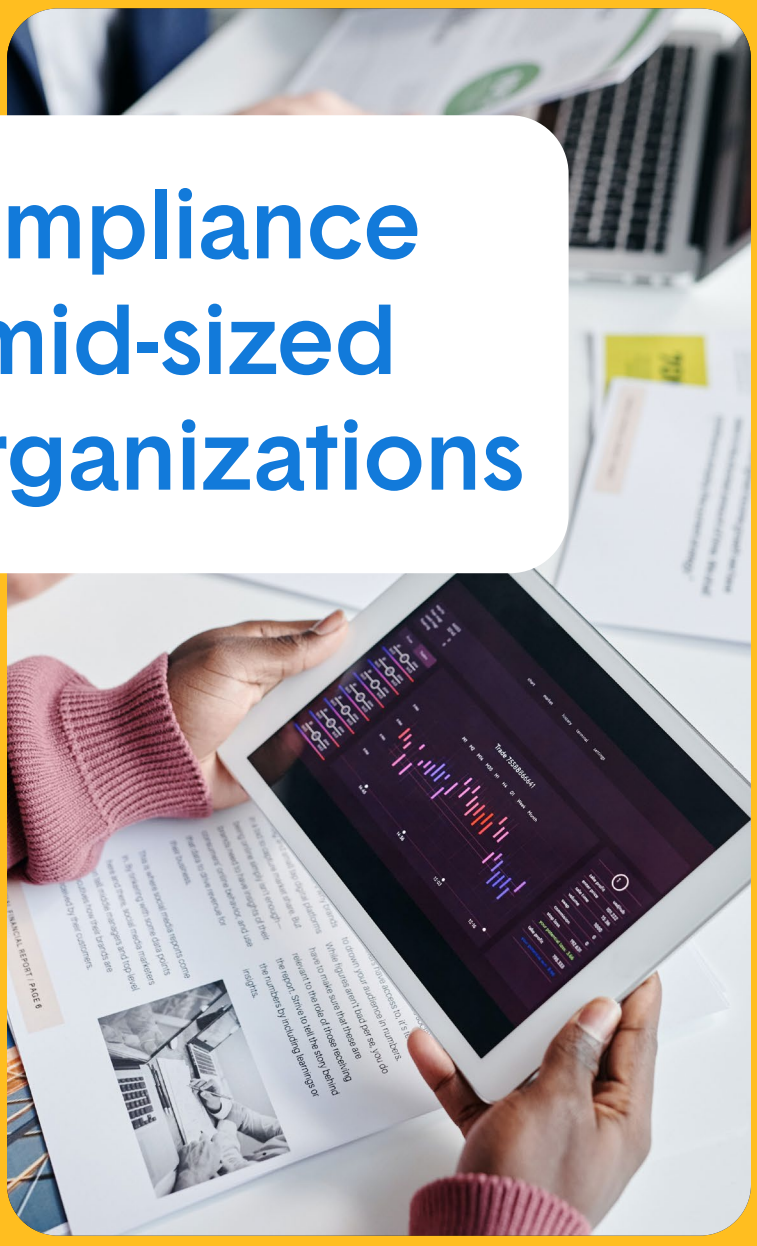
Thoropass™

Healthcare compliance for small and mid-sized technology organizations



thoropass.com →

Healthcare compliance has been the subject of much debate for as long as health and human services have existed in the United States and across the globe. While we could sit here and go over the myriad intricacies of laws in the healthcare industry, it would be wiser (and more time efficient) to discuss the impact patient data can have on your organization.

Healthcare organizations are constantly hit with cyberattacks that leak patient information. While larger insurance conglomerates might be able to weather the storm and pay off millions of dollars worth of fines, smaller and medium-sized companies simply don't have this luxury.

Developing a healthcare compliance plan in coordination with the progress and scale of your technology can ensure your processes are built to last. You'll have the net benefit of protecting patients while protecting your reputation without having to pay fines.

What defines a HealthTech company?

First, let's dive into what we're referring to as 'healthcare' technology companies (or HealthTech, for short.) The HealthTech landscape is far-reaching and can be divided into four main areas:

- **Telehealth**, which includes specialty fulfillment and telemedicine solutions, home testing and home health solutions, and online primary and general care services.
- **Digital therapeutics and digital treatments** encompass things like digital prescription services, VR treatments and therapies, neurological and brain health solutions, and chronic condition management.
- **Health coaching and wellness**, which include solutions for the treatment or management of alcohol and substance abuse, nutrition and weight loss, heart health and cardiac rehab, and pain and PT.
- **Digital care management** encompasses areas like AI care management tech, care search tools, health benefits navigation and so much more.

When it comes to healthcare compliance for small and mid-sized tech companies, the most impactful certifications will be HIPAA, SOC 2, and HITRUST. Below, we give an overview of each and make recommendations on choosing the best framework for your organization.

Understanding HIPAA compliance

When we think of healthcare compliance requirements for healthcare business associates and covered entities in the United States, the rules and regulations are seemingly endless. When it comes to patient data specifically, the primary regulation to be concerned with is HIPAA.

HIPAA, or the Health Insurance Portability and Accountability Act, was developed to protect PHI or Patient Health Information in any form like paper or stored in digital locations such as EHR (Electronic Health Records). Organizations that comply with HIPAA must comply with the law's privacy, security, and breach notification rules.

***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.*

Complying with the laws set forth by HIPAA is not an option, but a requirement to conduct business that uses patient data. Failing to comply can result in significant reputational and financial damage.

Components of HIPAA compliance: A breakdown of key elements

Several components make up an effective HIPAA compliance program:

Dynamic compliance roadmap

Static compliance roadmaps almost always find themselves colliding head-on with current regulatory standards. Conducting regular risk assessments to uncover PHI vulnerabilities can improve your security controls. Additionally, developing a plan that consists of course-correcting after a breach can keep your systems and processes stable in relatively unstable environments.

A dynamic compliance roadmap also involves training all employees that handle PHI as a significant portion of their job requirement. Comprehensive training should cover best cyber hygiene practices considering modern cyber threats from phishing, ransomware, and malware.

Alignment with Health and Human Services and Federal Trade Commission

Healthcare compliance programs revolve around Business Associate Agreements (BAAs) that establish agreements with third-party vendors in creating, receiving, maintaining, or transmitting PHI on behalf of covered entities and business associates. These agreements must thoroughly define the requirements to safeguard PHI and remain compliant with HIPAA.

Business associates with many different healthcare providers and payer organizations should work with their business partners to ensure HIPAA-related policies, procedures, incident reports, and risk assessments are organized accordingly.

Having digital or physical copies on hand can help ensure quick investigations from key regulatory bodies, including:

- OCR (Office of Civil Rights) operating under the HHS (Department of Health and Human Services)
- State attorney generals
- The FTC (Federal Trade Commission).

Compliance officers

Becoming HIPAA compliant is meaningless without any kind of enforcement of that compliance. Hiring a privacy officer—like a data protection officer or a security officer—or a CISO (Chief Information Security Officer) are key components of the HIPAA Security rule. In the absence of either, the CEO becomes the defacto administrative figure.

- **Privacy Officer**: This individual should oversee and manage privacy (or data protection) efforts. They are knowledgeable about regulations and can act as a point of reference whenever questions might arise.
- **Security Officer**: Security officers can ensure the confidentiality, integrity, and availability of PHI. They can implement safeguards to protect PHI from unauthorized access and address potential security breaches. They can also form a secondary stopgap to adequately train employees that need to handle PHI regularly.

The coming together of these different components is key to building a system that allows the organization to safely leverage patient information without compromising it. For the best results, it's best to approach these elements through a framework implementation that ensures policies and procedures are implemented and maintained throughout the many changes in the industry.

Understanding SOC 2 for healthcare compliance

According to the AICPA, SOC 2 (Service Organizations: Trust Service Criteria) aims to provide service management, user entities, business partners, and other parties with information about controls at the service organization relevant to security, availability, processing integrity, confidentiality, or privacy to support users' evaluations of their own systems of internal control.

Businesses of all sizes use SOC 2, but US-based startups tend to seek it out as a first step in their compliance journey.

There are five types of SOC reports:

- SOC 1: Service Organization Control 1 evaluates the effect of service organization controls on financial statements.
- SOC 2: Service Organization Control 2 is a procedure that examines service providers. The audit determines if they are securely managing 3rd party data, like personal information, to protect information and ensure privacy. Compliance with SOC 2 is usually a requirement when considering SaaS providers.
- SOC 3: Service Organization Control 3 is a public report of internal controls over security, availability, processing integrity, and confidentiality.
- SOC for Cybersecurity. To provide general users with useful information about an entity's cybersecurity risk management program for making informed decisions.
- SOC for Supply Chain. To provide specified users with information about the controls within the entity's system relevant to security, availability, processing integrity, confidentiality, or privacy to enable users to better understand and manage the risks arising from business relationships with their supplier and distribution networks.

Depending on your solution offering, SOC 2 can be valuable or even required for HealthTech companies to pursue. If you're dealing with personal health information, incorporating SOC 2 into our compliance program can be a pragmatic and proactive decision, given the overlap in controls and trust it can build with investors and buyers.

Components of SOC 2: A breakdown

SOC 2 audits are conducted based on two components: Trust Services Criteria and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework. Auditors require organizations to comply with all components of the COSO framework. Having said that, you only need to work toward the Trust Services Criteria that make the most sense for your business and its prospects.

Trust Services Criteria

Trust Services Criteria (TSC) are the five segments an auditor can test against when your organization starts toward a SOC 2 report. The five TSCs are security, availability, confidentiality, privacy, and processing integrity.

- Security focuses on protecting information and systems against unauthorized access, testing if your customers' information is protected at all times.
- Availability ensures secure and reliable access to systems for customers, validating uptime and demonstrating reliability.
- Confidentiality handles and protects designated confidential information, guiding identification, protection, and destruction.
- Privacy securely collects, stores, and handles personal information, testing effective protection.
- Processing Integrity ensures accurate, authorized, and timely service delivery while addressing processing errors, data storage, and maintenance.

Of the five TSCs, only security is required to complete your SOC 2 audit. That said, selling to enterprise organizations like hospital networks and insurance providers may come with greater expectations.

For HealthTech organizations, incorporating confidentiality criteria into your SOC 2 scope will be essential for holding up in those more sophisticated procurement processes. Additionally, if your organization is pursuing HIPAA and handles PHI, privacy can be another criteria to include to mitigate your organization's risk and demonstrate trust with potential buyers.

COSO framework

Unlike the Trust Services Criteria, the COSO framework provides guidance for strict, internal controls that all businesses are responsible for implementing when working toward SOC 2.

Specifically, the COSO framework requires organizations to address the following when it comes to internal controls:

- **Control environment**: The set of standards and processes that inform how controls are carried out throughout your HealthTech company. These standards ensure that your controls comply with applicable laws, protect your assets, and enable you to run your business efficiently.
- **Risk assessments**: Ostensibly, how your organization determines risk management. When controls face a risk, how will your organization assess and respond to the impact of that risk?
- **Control activities**: Generally set within the control environment, these activities define how your organization will mitigate risk and work toward the goals of your internal controls.
- **Information and communication**: How does your business communicate what's expected of its employees and controls internally and externally?
- **Monitoring activities**: The defined actions taken to evaluate and verify that controls are being upheld and functioning in your organization.

While a required component of implementing SOC 2 compliance, the COSO framework provides a significant value-add for HealthTech organizations, specifically regarding reducing and deterring fraud, protecting health information, and assessing other key compliance factors. When data is a pivotal part of your business's value proposition, anything that aids in its protection can be a differentiator in procurement and to potential investors.

HITRUST certification as a key differentiator in healthcare compliance

The HITRUST Common Security Framework (CSF) is a globally utilized and recognized framework with dozens of authoritative sources covering multiple industries. The CSF unifies and harmonizes many authoritative sources, pre-existing security regulations, and frameworks—such as NIST, HIPAA, ISO 27001, FedRAMP, PCI DSS, GDPR, and dozens of others.

Having expanded its reach considerably since its inception 16 years ago, the company has branched out from its sole focus in the healthcare industry, with countless other industries now adopting its methods. The HITRUST CSF assurance programs and frameworks are relevant to international organizations of all sizes.

While HIPAA is table stakes for HealthTech companies handling personal health information, HITRUST can provide unmatched levels of trust, especially with large insurance companies or hospital networks that need to mitigate vendor risk.

Components of HITRUST certification

HITRUST can be a long and intense process, but it will reap dividends. The following is a breakdown of the main components of the assessment process.

Readiness assessment options

All three tiers of HITRUST validation call for many levels of assessment to receive a completed report. The report ultimately helps companies improve their security posture and allow for greater stakeholder confidence.

- **r2 (risk-based two-year certification)**: The most comprehensive of the three, r2 is the original version of the certification and also the most intensive (and expensive!)
- **i1 (implementation one-year certification)**: Originally developed as the gateway to r2, the i1 tends to be the most commonly recommended version.
- **e1 (essentials one-year certification)**: The newest and most accessible certification with the fewest controls. The e1 serves as a great foundation for achieving future HITRUST certifications.

CSF control categories and objectives

Depending on the assessment option your organization chooses to pursue, the scope of controls your organization needs to take on will also change. Specifically, there are 14 HITRUST CSF control categories with 49 objectives and 156 control references (135 for security and 21 for privacy.), Each category has a designated objective (desired result) and multiple specifications (policies, guidelines, practices, etc.).

There are up to three levels of implementation for control requirements, and there are over 1,900 requirement statements within the HITRUST CSF. However, based on risk and regulatory requirements, only a subset of the total list will be in scope for your organization.

Validated assessment

The HITRUST Alliance vetted and approved External Assessor firm you choose will highlight gaps in your security and provide recommendations to fix your processes and controls according to your chosen assessment level. As you get closer to mitigating these gaps in coordination with close reviews from the external assessor, you will move directly into HITRUST CSF validation.

If you pass the final review by the HITRUST Assurance Team, and score high enough within the validation, you will then be issued your letter of certification. Your report will only be 'certified' if it meets specific scoring criteria.

Customizing your healthcare compliance program

The larger you become and the more data you take on, the greater the impact an unexpected disaster can have. That is why it is wise to develop an effective healthcare compliance program quickly rather than deal with the consequences later when you have a world-ending amount of data.

Creating a customized program for healthcare-covered entities and business associates will naturally revolve around complying with HIPAA, SOC 2, HITRUST, or a combination of the three. Implementing policies and procedures that enhance the ongoing security of PHI in response to constantly changing healthcare regulations is critical. Building an ever-evolving compliance roadmap that involves all employees across organizational functions is key.