How HITRUST Certification Can Help You Ensure HIPAA Compliance

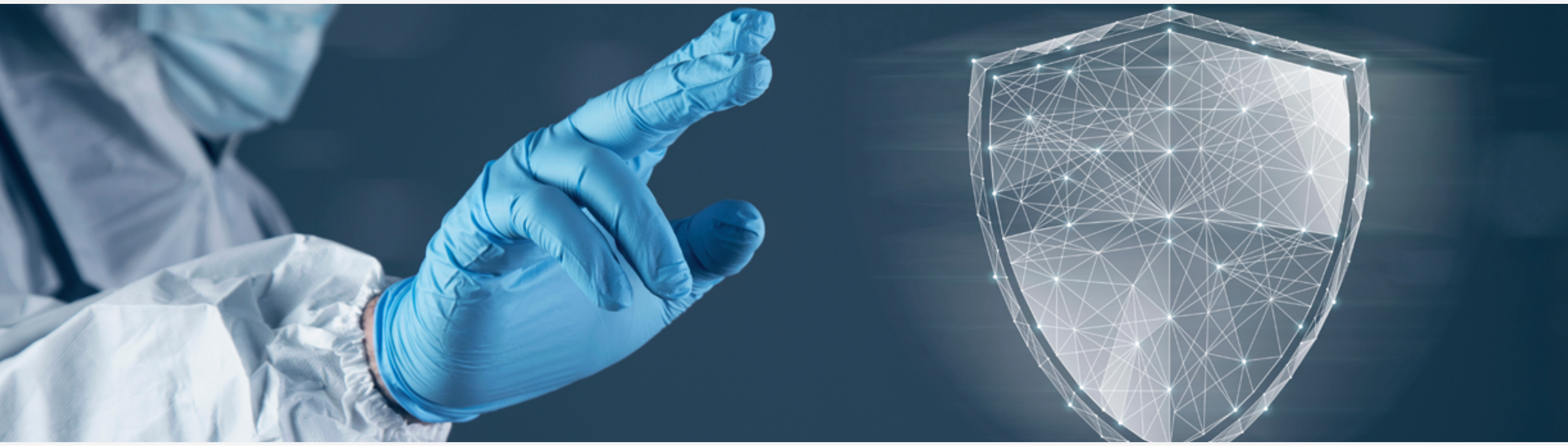
If you work in the healthcare industry, you're aware of a long list of acronyms that are part and parcel of your chosen profession. Two of the most critical ones are HIPAA and HITRUST. While there are many safeguards you can take to protect your healthcare practice (such as physical, administrative, and technological), doing so effectively requires a nuanced approach — one that can be so complex as to require full-time attention around the clock.

You can hire a dedicated team to take care of it. You can conduct regular audits. You can create extensive processes and instruct your teams to undergo extensive training programs. Yet, as businesses scale, cutting-edge technologies are released, and cybercriminals become more sophisticated, it can feel like a never ending and exhaustive quest.

It is precisely due to these realities that HITRUST Certifications were developed. But before looking into what the process entails, it's imperative to thoroughly understand the current landscape of cybersecurity within the healthcare industry.

Recent FTC Safeguards Rule Amendments

Cybersecurity is always a crucial component of any industry — of any facet of life, really. We've all become accustomed to storing sensitive data online for convenience, easy access, and portability. This is why no matter the electronic device you're using, you're likely aware of taking certain precautions to keep your information secure.



This need for safety measures increases exponentially when handling healthcare information. In addition to keeping patients' data confidential to prevent issues such as identity theft, this type of information could also expose individuals to embarrassment and discrimination. And depending on what's disclosed, it could also carry a stigma that follows the patient's life long-term.

To add insult to injury, security breaches are slated to result in approximately $10.5 trillion in losses every single year by 2025. And healthcare organizations are leading the country in data breaches. As if that weren't problematic enough, medical identity theft is expected to continue to increase dramatically.

Healthcare providers are especially prone to targeted attacks by cybercriminals because patient information can be used to commit insurance fraud. Not only is this costly for individuals and entities, it's also disruptive to patient care — affecting both their finances and, most importantly, their health.

Information that facilitates this criminal activity includes using patients' names, social security numbers, medications and treatments they are undergoing, health insurance account numbers, and Medicare or Medicaid numbers.

As such, it's imperative for healthcare providers to ensure that patient information remains confidential, both while in transit and while at rest. End-to-end encryption is more crucial than ever, but that's just the tip of the iceberg. Federal law requires compliance with a long list of requirements to safeguard patient data, and failing to comply with it will cost you your reputation, significant amounts of money, and even your ability to continue offering services within the healthcare industry.

HIPAA violations can also result in criminal penalties. Penalties can be as much as $250,000 per violation, restitution to the victims, and jail time.

Who is held responsible and to what extent depends on factors such as whether there was a lack of adequate training, negligence, or whether an act was willful? Prosecutors will also consider the extent of the damage caused to patients.

No matter how you look at it — or how busy you are — HIPAA compliance should always be a priority.

What is HIPAA?

The HIPAA acronym stands for the Health Insurance Portability and Accountability Act. It's a federal law that establishes standards that certain entities need to comply with in order to keep protected health information (PHI) from being disclosed without patient consent.

That said, this law is often misunderstood. A significant segment of the population seems to think that the act forbids the disclosure of health-related information across the board. That's not exactly how it works. It also requires a lot more than simply keeping data confidential. In an age where everything is online and done electronically, it makes it imperative for covered entities to be proactive about cybersecurity.

Who is Required to Comply With HIPAA?

First things first. HIPAA applies to specifically defined covered entities. These include:

01 **Healthcare Providers**

This category includes every single healthcare organization, regardless of its size. As long as they store and/or transmit health data electronically, they are required to comply with HIPAA.

02 **Health Insurance Plans**

This includes anyone who provides full or partial payment of healthcare costs, regardless of whether it's an HMO, Medicare, Medicaid, employer-sponsored insurance, and government subsidies.

03 **Health Business Associates**

This includes any individual or organization that performs job duties for a healthcare organization — administrative functions, data analysts, billing, and anyone else who enables healthcare organizations to run efficiently.

04 **Healthcare Clearinghouses**

These are entities that act as middlemen who process and route claims between healthcare organizations and health insurance providers.

None of these entities can disclose patient information unless they receive express consent, in writing. In addition, HIPAA establishes that patients have the right to obtain copies of their health records, as well as to direct covered entities to send their PHI to third parties.

It's also important to know that each State may also implement its own laws regarding patient confidentiality. However, if there's a contradiction between laws, HIPAA supersedes State laws.

Exceptions to HIPAA Confidentiality Requirements

Now, as with most things in life, compliance with HIPAA's confidentiality requirements is not absolute. There are a handful of exceptions when a covered entity may disclose a patient's protected health information:

- A public health authority that is authorized by law to collect the information to prevent or control a disease, injury, or disability. An example of this scenario would be reporting a medical condition to public health investigations.
- A person subject to the jurisdiction of the United States Food and Drug Administration (FDA), who is collecting data related to the quality, safety, or effectiveness of an FDA-regulated product. An example would be transmitting information regarding the reported side effects of a medication.
- To enable medication and/or product recalls.
- When a healthcare provider reasonably believes that injuries are the result of child abuse or neglect.
- When a healthcare provider reasonably believes that injuries are the result of domestic violence.
- To prevent serious harm to the patient (self-harm) or to potential victims the patient has expressed a desire to harm.
- To assist in the investigation of crimes, licensure, or disciplinary actions against
- To prevent or control disease, public health investigations, and public health interventions.

HIPAA Concerns With Modern Technology

As technological advances continue to make life easier and more convenient, there are additional considerations to keep in mind regarding how to protect PHI.

Telehealth

Telehealth is defined as providing remote healthcare via electronic communications. While certain medical conditions require in-person visits and treatment, follow up consults and discussion of other ailments can be done with the use of video teleconferencing.

While telehealth has existed for several years now, it has become exponentially more prevalent in a post COVID-19 world; and it is imperative to utilize software that is HIPAA compliant. Some of the features you'll want to implement include:

- End-to-end encryption
- Remote monitoring
- Automatic log-off when not used for a specific timeframe

Social Media

HIPAA was enacted long before social media channels were a cultural staple. However, these platforms provide healthcare providers to engage with patients and people within their community with regularity. You can still promote your services and answer general questions through Facebook, Instagram, TikTok, LinkedIn, etc…, but it is of utmost importance to refrain from sharing any kind of PHI.

Also, be mindful of never including photos of patients to show progress or before and afters — even if they remove any identifiable features. By the same token, do not feature your facilities with patients in them. If you opened a new office or remodeled a location, or simply want to showcase what visitors can expect, use photos of empty spaces, or ask any employees if they'd like to participate.

Further, train your staff to follow these rules — both when using your facility's social media pages, as well as their personal ones. And if a patient initiates a conversation and voluntarily discloses PHI, delete anything posted publicly, and reroute their conversation to a safer platform (like your patient portal).

Text Messaging

Text messages aren't encrypted. Users also use this feature while connected to unsecure public networks. Therefore, while healthcare providers may (and do) communicate with patients using SMS to send appointment reminders, it is advisable to send communications that link to secure portals with login information and data encryption.

What is HITRUST Certification?

Now that you have a better understanding of HIPAA requirements and who's required to comply with them, let's take a look at a tool that was specifically designed to help healthcare providers and other covered entities uphold their confidentiality obligations.

The Health Information Trust Alliance (also known as HITRUST) is a non-profit organization that developed a framework that safeguards sensitive information. When you implement it, you get the peace of mind that comes with ensuring that you're complying with federal regulations.

HITRUST is used by entities that are required to adhere to a long list of laws, including the California Consumer Privacy Act (CCPA), General Data Protection Regulation (GDPR), and the Federal Information Security Modernization Act (FISMA), among others. And of course, with the Health Insurance Portability and Accountability Act.

When you get a HITRUST certification, you become well-versed in every single security control you need to implement to prove compliance with local, industry, and federal regulations. Furthermore, since it is widely accepted as the gold standard of entities that are in full-compliance, it also demonstrates trustworthiness.

The certification process can take between nine months to a year, and it involves going through three phases:

Readiness Assessment

During this stage, organizations look at their policies, processes, risk management, security implementation, and how everything is measured.

Security Controls Remediation

During the remediation process, you are required to make all necessary changes to mitigate risks and patch vulnerabilities. This may also entail creating new processes.

Certification Audit

During the final stage, you measure your organization's compliance with HITRUST Common Security Framework (CSF).

These evaluations are performed by an external HITRUST assessor. Once you either meet or exceed the CSF requirements, you receive certification.

HIPAA and HITRUST

While HITRUST is used by a wide array of industries to ensure regulatory compliance, it is especially useful within the healthcare arena.

Having a HITRUST means that you can focus on running your practice — or any element relating to a healthcare provider's operations — without wondering whether you're at risk of HIPAA noncompliance. It's also an efficient way to run your operations long-term, since using the HITRUST approach means that you can scale with confidence, without worrying about modifying your compliance processes.

In fact, the vast majority of covered entities in the United States use the HITRUST framework to ensure that they are adhering to all privacy requirements. So while it is common to find content on search engine results pages with titles about HIPAA vs. HITRUST, know that it is not a matter of one versus the other. HIPAA is the federal law, and HITRUST is the methodology that makes it more feasible and practical to comply with it.

About SCA and Our HITRUST Approach

The process of getting ready for and obtaining HITRUST certification is long, complex, and can very often become overwhelming — especially since a covered entity's primary focus is on actually performing its every day duties.

At SCA Security, we help organizations successfully prepare for every single stage, so that you can be ready for the certification audit. If you have any concerns, questions, or want to receive guidance from industry-leading experts, we're ready to help.

We have over 15 years of experience specializing in information security programs that comply with HIPAA and other federal and state regulations.

Contact us to prepare for your HITRUST certification. We'll become an extension of your team as we get you ready to do this right.

Protect Your Data