CLEARDATA

What You Need to Know About HITRUST Certification

With HITRUST Certification a healthcare organization signals to business partners and regulatory agencies that protection of sensitive information is both a necessity and a priority, that essential security and privacy controls are in place, and that management is committed to information security and privacy.

r2 RISK-BASED 2-YEAR HITRUST® CERTIFIED

Among all the things healthcare companies expect of you as they move their patients' protected health information (PHI) from on-premise into the cloud, HITRUST certification is one of the most important.

> **That's because in an age of unprecedented security risks and a seemingly never-ending list of regulatory requirements, HITRUST certification is the gold standard when it comes to healthcare information security and assurance.**

It's a way of not only protecting your customers' data, but also ensuring that they remain compliant with all of the regulations affecting the healthcare industry, thus reducing your risk to the lowest level possible.

HITRUST offers both a HITRUST Implemented 1 year (i) certification, as well as the risk-based 2-year (r2) assessment that provides the highest level of assurance, which we will be outlining in this document.

What is HITRUST?

The **Health Information Trust Alliance** (HITRUST) was born out of the belief that information security and privacy should be a core pillar of the broad adoption of health information systems and exchanges. Working in collaboration with healthcare, business, technology, and security leaders, HITRUST established the HITRUST Common Security Framework (CSF), a certifiable framework for organizations that create, access, store, or exchange personal health and financial information.

Fundamentally, HITRUST is an information security framework for the healthcare industry. It brings international, federal, state, and third-party regulations and standards together into a holistic set of controls designed to protect healthcare data. More specifically, it provides a clear and measurable benchmark for identifying hosting and cloud computing vendors that meet the highest standards of HIPAA compliance.

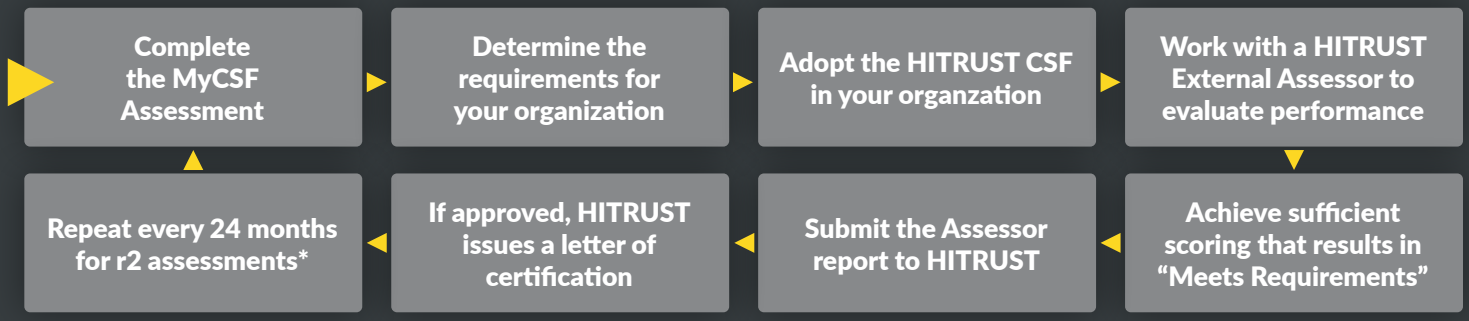
But it doesn't just support HIPAA compliance. With a HITRUST certification, you can more easily demonstrate compliance with regulations such as HIPAA, CMS, GDPR, FTC, and state laws, including alignment with standards and frameworks like ISO 27001, NIST CSF, CIS CSC, and PCI DSS among others. As a result, rather than being concerned about whether your third-party partners have met the many standards individually, HITRUST certification ensures that your partners are compliant with all of them, while eliminating the variability in the definition of acceptable security requirements.

Now that we know what HITRUST is, let's look at what getting certified entails.

HITRUST Certification is the foundation for compliance...

- ✓ HIPAA
- ✓ GDPR
- ✓ PCDI-DSS
- ✓ ISO 27001
- ✓ COBIT
- ✓ NIST
- ✓ FTC
- ✓ Local Laws

The Path to HITRUST Certification



** Includes interim assessment after 12 months*

To achieve HITRUST certification, you must successfully demonstrate that your organization meets all of the controls in the CSF required for the current year's certification. Not only that, you must do so at the appropriate level required for your specific organization based on your responses to the MyCSF self-assessment tool requirements statements. In addition, you must achieve sufficient scoring that results in "Meets Requirements," based on the maturity level scoped for the assessment.

Practically speaking, this is a lot easier said than done. Organizations who are well-prepared require anywhere between six and nine months to get certified. Meanwhile, for some organizations, the process to develop and implement the corresponding controls, mechanisms, and technologies to support each of the CSF requirements could cost hundreds of thousands of dollars, based on the development resources and controls needed for the company. Having said that, it's often worth the effort. Not only does HITRUST certification bring prestige to organizations, HITRUST certification is an industry-leading certification that HCOs increasingly expect from their partners.

Payers and Providers Trust HITRUST

HITRUST is a clear indication that you have essential security and privacy controls in place, and that your management team is committed to privacy and information security. As a result, certain healthcare organizations such as Anthem, Health Care Services Corp., Highmark, Humana, and UnitedHealth Group all require certification from their partners.

If you want to do business with payers and providers, a HITRUST certification is almost always nonnegotiable. Not only that, being certified can also help shorten sales cycles by streamlining the diligence process and making conversations with Chief Information and Security Officers easier.

Alternatively, companies that want to accelerate their HITRUST journey can partner with providers that allow for HITRUST inheritance. In that way, they can adopt their provider's scores on approved controls, as part of their assessment journey. It's also possible simply to work in a HITRUST certified environment. In such instances, your company will not have gone through all of the hoops necessary to become certified but will still get many of the benefits HITRUST brings.

> With HITRUST CSF certification, you signal to your business partners and other third parties that you've made protecting sensitive information a priority.

The bottom line is, if you're unsure how best to approach HITRUST, the best way to move forward is simple: Partner with ClearDATA, the leading cloud platform provider with HITRUST certification for healthcare.