logicworks

HITRUST™ ON THE CLOUD

Navigating Healthcare Compliance

As the demand for digital health solutions increases, the IT regulatory landscape continues to evolve. Staying ahead of new cybersecurity rules and regulatory changes gives your company a competitive advantage — and also helps avoid costly fines and reputational damage.

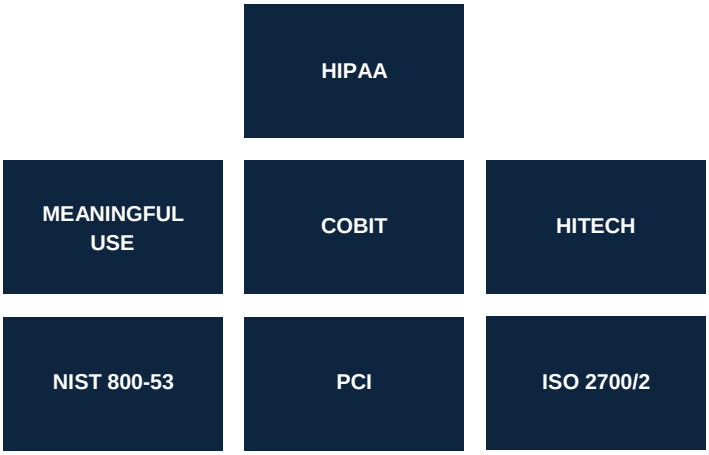
The HITRUST CSF™ is a widely adopted security framework for healthcare companies and has been gaining popularity as a more structured, unified, and comprehensive standard that can be used to help satisfy HIPAA and HITECH in a defensible fashion. However, many small and mid-sized healthcare companies struggle with understanding the framework and building an internal review and certification program, particularly if they have recently migrated to the cloud.

Matthew Sharp, CISO of Logicworks, and his team have helped many clients understand HIPAA and HITRUST™. Below, they respond to the most frequently asked questions. Logicworks is a compliant cloud solutions provider that helps companies like Orion Health, MassMutual, and dozens of healthcare SaaS companies to build and manage public, private, and hybrid clouds. Contact Matt for more information.

WHAT IS HITRUST™?

HITRUST is a privately held corporation established by a coalition of leaders across a variety of healthcare organizations, including Anthem, Humana, and UnitedHealth Group. They developed the HITRUST CSF™ that includes a prescriptive set of controls incorporated from multiple standards, regulations, and business requirements.

In June 2015, several of the largest adopting organizations announced that in roughly two years, they would only work with Business Associates that had achieved HITRUST CSF™ certification. This has caused a dramatic rise in interest in the HITRUST CSF™, particularly for software and digital health companies who sell services to these companies.



The Building Blocks of HITRUST CSF

As a result, some companies that are currently becoming HITRUST Certified "must" do so in order to remain competitive. However, some payers and providers adopt HITRUST CSF™ because it provides a prescriptive, streamlined process for implementing and assessing a cybersecurity program that protects electronic personal health information (ePHI).

WHAT IS HIPAA AND HOW IS IT DIFFERENT FROM HITRUST™?

Comparing HIPAA and HITRUST™ is like comparing apples and oranges; HIPAA is a law, and HITRUST CSF™ is a framework. The HITRUST CSF™ integrates the requirements of the HIPAA Security Rule with the standards of NIST, HITECH, PCI DSS, and other controls, facilitating a unified control rationalization. The HITRUST CSF™ offers a Validation/Certification program — a clear, prescriptive set of controls for achieving compliance, and a toolset to support assessment. Unlike HIPAA, your organization can be “HITRUST CSF™ Certified”. The benefit of HITRUST™ assessment is that you can “assess once and report many” – in other words, that a single HITRUST™ assessment can produce a HIPAA assessment report, SOC 2® report, NIST assessment report, etc.

Therefore, in order to produce a HIPAA assessment report, either for internal purposes or to demonstrate compliance to customers, you have two options: either go through the HITRUST™ assessment process, which can produce a HIPAA assessment report and potentially many other reports (such as SOC 2 or NIST), or go through a HIPAA assessment process, which produces a HIPAA assessment report.

The following table highlights the differences between HITRUST CSF™, HIPAA, and other frameworks.

CONSIDERATION	HITRUST CSF™	HIPAA	PCI-DSS	NIST	ISO
Comprehensive - General Security	✓	Partial	✓	✓	✓
Comprehensive - Regulator, Statutory, Business Requirements	✓				
Prescriptive	✓		✓	✓	Partial
Risk-Based (Rather than Compliance-Based)	✓	Partial	Partial	✓	✓
Practical and Scalable	✓	✓			
Supported and Maintained by 3rd Party	✓		✓	✓	✓
Vetted by Industry Experts	✓			✓	✓
Open and Transparent Update Process	✓		✓	✓	✓
Audit or Assessment Guidelines	✓		✓	✓	✓
Consistency and Accuracy in Assessment/Evaluation	✓		Partial	✓	Partial
Certifiable	✓		✓		✓
Assess Once and Report Many	✓			Partial	Partial

Source: HITRUST Alliance

IF I'M HITRUST CSF CERTIFIED, DOES THAT MEAN I'M HIPAA COMPLIANT?

The short answer is yes. According to HITRUST, the HITRUST CSF™ is equal to credible HIPAA compliance. More specifically, "[by] implementing the HITRUST CSF™ control requirements that are applicable to an organization based on its specific organizational, system and regulatory risk factors, each and every standard and implementation specification in the Security Rule is addressed in a very complete and robust way."

HITRUST states that the HITRUST CSF™ certification has been previously accepted by the OCR as supplementary evidence of compliance with HIPAA.

WHAT IS THE HITRUST CSF™ CERTIFICATION PROCESS?

Most companies begin the process by hiring an external risk management advisor and assessor to walk them through the HITRUST™ certification process. At that point, the process is divided into these main steps:

1. **Scoping:** You determine your level of risk based on factors like number of employees, number of PHI records, mobile phone usage, etc. in the HITRUST MyCSF™ platform. The platform then generates a certain number of requirements that map to 19 separate "domains".
2. **Self-Assessment:** You upload documentation and conduct a self-assessment against your specific requirements. If you are working with an external risk management advisor, they will review your self-assessment to advise you of areas where you over-scored/under-scored yourself and suggest paths to remediation.
3. **Remediation:** Remediation: Based on gaps exposed in the self-assessment, your team remediates policies, processes, and procedures.
4. **Validated Assessment:** A HITRUST CSF™ Approved Assessor conducts a formal review of documentation loaded into the HITRUST MyCSF™ portal. Once the validated assessment begins, no changes or updates can be made. The assessment will be validated by interviews, requests for samples, and other tests.
5. **Corrective Action Plan (CAP):** For every requirement that receives a score below 71.00, you need to submit a CAP, which consists of a written plan for remediation (including timeline and responsibilities.)
6. **Reports & Certification:** If you receive an average score of 62.00 or greater across all requirements in each domain you will receive a Certified Report (i.e., you will become HITRUST CSF™ Certified). If you receive an average score of below 62.00 for ANY of the domains, you will receive a Validated Report but will not be HITRUST CSF™ Certified.
7. **Interim Assessment**: A Certified Report is valid for two years as long as you undergo an Interim Assessment within 12-14 months of your initial report, along with meeting certain other requirements which are defined in the Certification Letter.

It is highly recommended that you conduct a Self-Assessment prior to starting the validated assessment process. Conducting a Self-Assessment allows your team time to review requirements and remediate before conducting the “real” assessment, as it would be a tremendous loss of time and funds to go through the process only to discover that you fall just short of receiving a HITRUST™ CSF Certified Report.

Individual requirements are scored in 5 Maturity Levels: Policy (weighted 25%), Process (25%), Implemented (25%), Measured (15%) and Managed (10%). The average requirement score for each domain is multiplied by its weight to generate your domain score. Receiving a domain score of less than 62.00 in just one domain (out of 19) will mean that you fail HITRUST CSF™ Certification. To become HITRUST™ Certified without CAPs (Corrective Action Plans), each requirement must have a score of 71.00 or greater.

IN REAL TERMS, WHAT IS IT LIKE TO GET HITRUST CSF™ CERTIFIED?

The process varies depending on the size and complexity of your organization, but we can provide a quick example.

Logicworks provides services to a healthcare startup that provides technology applications for multiple large health insurance plans. Our client has fewer than 50 employees and fewer than 5 IT staff members. Logicworks helped the company build their SaaS application on Amazon Web Services (AWS) in a manner that complied with both the HIPAA Security Rule and Amazon’s BAA in 2016. Logicworks now functions as an extension of their infrastructure operations team with 24x7 technical support, incident response, DBA support, etc.

Last year we jointly committed to obtaining HITRUST CSF™ Certification. This required that the client’s AWS environment be re-architected, a process that began with Logicworks and the company conducting an in-depth gap analysis of existing systems, and establishing requirement definitions for the future design. The process resulted in a new AWS environment, and included licensing of several additional security tools. The new environment cost about 20% more than their previous environment built to HIPAA standards. This was mostly as a result of using additional AWS services to satisfy security controls, refactoring to leverage HIPAA approved services on AWS, costs to develop additional automation for response, custom reporting, increased level of service, and the cost of additional security tools.

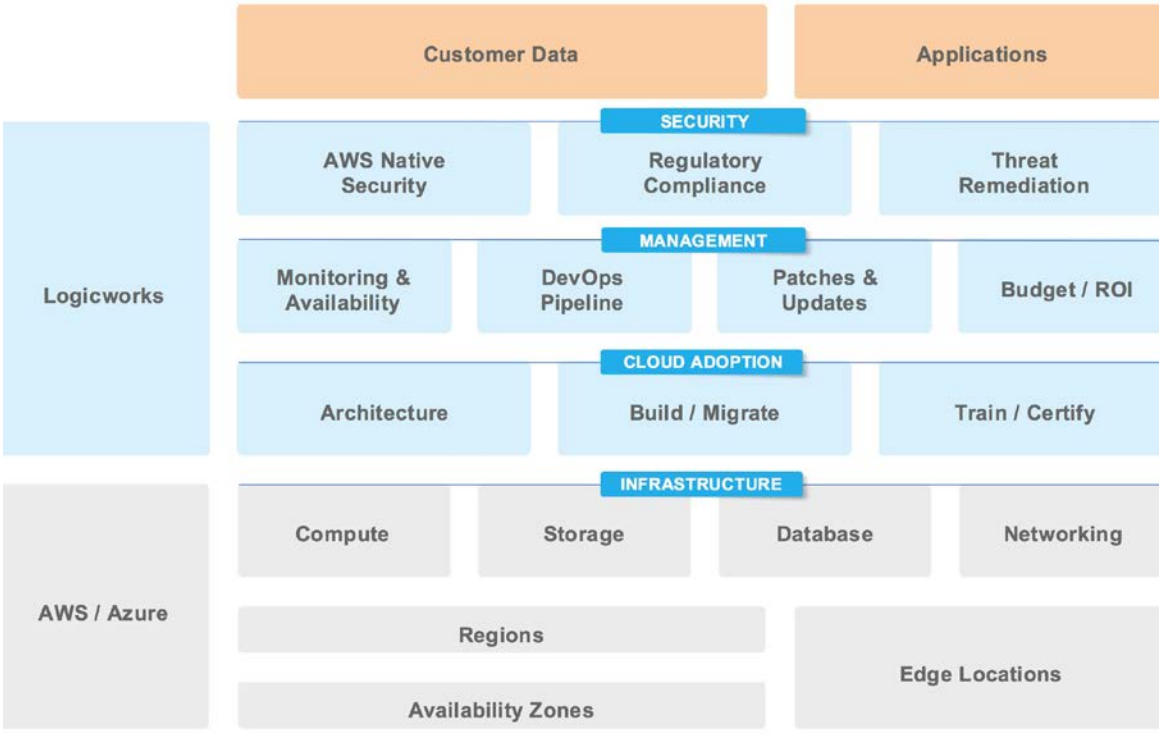
Based on a risk analysis, the company had to meet about 300 requirements during the HITRUST CSF™ Certification process. Of those 300 requirements, Logicworks was able to fulfill about 50% of the requirements, which resulted in a dramatic simplification of the compliance process for the company. Logicworks supplied extensive documentation and had several, in-depth conversations with assessors and helped coach both the assessor and the company through AWS services in order to clarify its documentation. The company successfully received a HITRUST™ Certified Report in March 2017. Without Logicworks, the audit process would have taken the company significantly longer, perhaps over a year. This efficiency was due to Logicworks' existing documentation, the maturity of its infrastructure security practices, and its experience building compliant systems on AWS cloud.

HOW IS HITRUST CSF™ CERTIFICATION DIFFERENT WHEN YOU'RE RUNNING ON IAAS (AWS, AZURE, GOOGLE COMPUTE)?

By migrating to AWS or Azure, customers have a shared compliance responsibility. This shared model means that the cloud provider manages the infrastructure components from the host operating system (virtualization layer) down to the physical security of their datacenters. It is the customer's responsibility to configure and secure provided services.

In other words, the cloud provider controls physical components; the customer owns and controls everything else. As AWS states repeatedly, "AWS manages security of the cloud, security in the cloud is the customer's responsibility." To learn more about managing compliance on AWS, download our free eBook.

HITRUST™ v9 includes FedRAMP Support for Cloud and IaaS Providers, including guidance for running a cybersecurity program on IaaS. This may help companies understand the cloud provider's responsibility model An experienced cloud compliance support company like Logicworks can also help provide a RACI chart that maps HITRUST™ controls to MSP responsibility, MSSP responsibility, AWS/Azure responsibility, and customer responsibility. HITRUST updates the framework at least once a year, so additional capabilities are forthcoming.



In some ways, IaaS can actually facilitate the process of implementing a robust cybersecurity program due to the availability of tools to automate certain controls. The abstraction layer afforded by public cloud providers empowers a clear use of automation, often driven via Infrastructure as Code (IaC) and purposeful orchestration. The powerful result is that clients can perfectly define the intended state of every environment. By doing so, they accelerate their ability to deploy micro changes in addition to patches and configuration updates while understanding and mitigating many of the risks associated with change. In Puppet's 2016 State of DevOps Survey, they found that high-performing IT teams recover from failure 24x faster than average IT teams.

Table 1: Changes in IT performance of high performers, 2016 to 2017

IT performance metrics	2016	2017
Deployment frequency	200x more frequent	46x more frequent
Lead time for changes	2,555x faster	440x faster
Mean time to recover (MTTR)	24x faster	96x faster
Change failure rate	3x lower (1/3 as likely)	5x lower (1/5 as likely)

Source: Puppet State of DevOps Report 2017

HOW CAN LOGICWORKS HELP ME ACHIEVE HITRUST CSF™ CERTIFICATION?

Logicworks is a compliant cloud solutions provider that helps healthcare companies build, automate, and manage AWS, Azure, and Hybrid clouds. We have 20+ years of experience working in healthcare organization. Additionally, Logicworks is annually assessed for HIPAA, PCI-DSS, and SOC 2. Logicworks is the only AWS Premier Consulting Partner with the audited Healthcare and Security Competency in both Security Consulting and Security Operations and Automation.

We can help organizations achieve HITRUST CSF™ Certification either through a consultative role or by acting as an ongoing infrastructure management partner. Logicworks Cloud Migration Services can help companies that want to move to AWS or Azure to understand how IaaS security controls map to specific compliance requirements, and help plan and build a compliant infrastructure solution. Our Cloud Management Services provide 24x7 engineering support, incident response, security management, and cost optimization for customers operating on AWS and Azure.

Customers that leverage Logicworks Cloud Management Services move to a shared compliance responsibility model between the cloud provider, Logicworks, and their internal teams. This reduces the operational burden of controlling the security telemetry and response and shifts the client into a role of governance and supervision.

HITRUST CSF™ Certification is not as complex as it may seem. Logicworks drastically simplifies the process by building and maintaining compliant systems that allow you to reduce the cost and risk of noncompliance. By leveraging Logicworks, our clients get to the cloud faster, operate in the cloud more efficiently, and do so with greater assurance.

Logicworks, the leader in compliant cloud solutions, provides end-to-end professional services, cloud management, and cloud security to clients in the finance, healthcare, and SaaS industries. For more information, please contact info@logicworks.com or (212) 625-5300.

logicworks

155 Avenue of the Americas, Fifth Floor | New York, NY 10013
P: 212.625.5300 | www.logicworks.com