Healthcare's Guide to

HITRUST Certification

CLEARDATA®

YOUR GUIDE TO

HITRUST

The Healthcare Security Benchmark

Organizations that handle sensitive information, whether it's protected health information (PHI) or personally identifiable information (PII), understand that prospective clients have high expectations for security and compliance standards.

HITRUST certification not only demonstrates industry standard security practices for protecting your customers' PHI, it also provides assurances for continuous compliance with healthcare regulatory requirements, frameworks, and standards.

Why Read this Guide?

- Simplify Your Cyber Risk Journey
- Build Trust with Your Patients and Partners
- Save Time & Resources

CONTENTS

What is HITRUST and Why Does it Matter?

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 information 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, reducing your risk to the lowest level possible.

Revealing unprecedented insights and performance data, HITRUST showcases a **00.64% breach rate** through its program, redefining excellence in information security.

But it doesn't just demonstrate assurances for HIPAA compliance. With HITRUST certification, healthcare organizations handling sensitive data can more easily comply with PCI-DSS, ISO 27002, NIST CSF and SP 800-53, and CIS CSC, as well as the growing number of state laws.

Rather than being concerned whether security and compliance practices adequately meet the needs of current regulatory and threat landscapes, adoption of the HITRUST CSF and certification reduces the need to align to multiple frameworks, enabling organizations to focus more on core competencies and specific business initiatives.

Who uses, recommends, and accepts HITRUST certification?

81%
of U.S. hospitals and health systems

83%
of U.S. health plans

75%
of Fortune 20 companies

Top 3
Cloud service providers

HITRUST vs. HIPAA

HIPAA Security Rule	The HIPAA Security Rule establishes national standards to protect electronic personal health information. Found at 45 CFR Part 160 and Subparts A and C of Part 164, this rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.
HITRUST	The HITRUST Common Security Framework (CSF) provides a comprehensive certification that incorporates various standards, including HIPAA and NIST, to ensure consistent data protection measures.

Understanding the HITRUST Certification Landscape

Knowing the distinctions between the different certification levels is important because they provide a roadmap for organizations to continuously improve their information risk management and compliance programs. Each level builds upon the previous one, ensuring that organizations are continuously addressing new challenges and evolving regulatory requirements. These certification levels — e1, i1, and r2 — can help organizations align their cybersecurity efforts with their specific needs and regulatory requirements. Let's take a look at them.

e1 HITRUST CERTIFIED

Entry-Level Assurance

The e1 certification is often considered the entry point into the realm of cybersecurity certifications. It offers a foundational level of assurance, covering basic security measures and protocols. Organizations pursuing the e1 certification are typically at the beginning of their cybersecurity journey, aiming to establish a baseline of security controls. This level is less rigorous compared to higher-tier certifications, making it accessible for smaller organizations or those new to implementing formal security frameworks.

i1 HITRUST CERTIFIED

Intermediate Assurance

Stepping up from e1, the i1 certification represents an intermediate level of cybersecurity assurance. It encompasses a broader range of security practices and requires more stringent adherence to security protocols. Organizations achieving the i1 certification demonstrate a more robust commitment to cybersecurity, often incorporating more advanced security measures and regular assessments to maintain compliance. This level is suitable for organizations with more mature security programs looking to enhance their security posture further.

r2 HITRUST CERTIFIED

Highest Level of Assurance

At the pinnacle of cybersecurity certifications is the r2 certification. Achieving r2 certification signifies that an organization has implemented comprehensive and advanced security controls, addressing a wide array of potential threats and vulnerabilities. The r2 certification involves extensive assessments, audits, and monitoring to ensure the highest level of security. Organizations with r2 certification are typically those with the most stringent security requirements, often in highly regulated industries where security breaches could have severe consequences.

Benefits of HITRUST for Healthcare

HITRUST certification serves as a gold standard for healthcare organizations striving to protect sensitive patient data while navigating a complex regulatory landscape. Here's how HITRUST can transform your organization.

1 Enhanced Trust and Credibility

Achieving HITRUST certification signals to patients, partners, and regulators that your organization is committed to the highest standards of data security and privacy. This certification acts like a seal of approval, reassuring stakeholders that robust measures are in place to safeguard sensitive information. As a result, healthcare companies can foster greater confidence among patients and partners, enhancing their overall reputation in the industry.

2 Simplified Regulatory Compliance

HITRUST offers a comprehensive framework that simplifies the daunting task of regulatory compliance by integrating multiple standards. This holistic approach ensures that healthcare organizations meet diverse requirements through a single, unified set of controls. By streamlining compliance efforts, HITRUST reduces the complexity and workload typically associated with adhering to various regulatory mandates, allowing organizations to focus on supporting or delivering quality healthcare, while ensuring patient safety.

3 Strengthened Risk Management

With HITRUST, risk management can become a more structured and manageable endeavor. The framework provides clear benchmarks for improving processes for identifying potential threats and vulnerabilities, while positioning organizations to implement effective mitigation strategies. By adhering to HITRUST's comprehensive security controls, healthcare companies can proactively address risks, reducing the likelihood of data breaches and associated penalties. This proactive stance not only protects patient data but also safeguards the organization's financial and operational health.

4 Competitive Advantage

In a competitive healthcare market, a HITRUST certification can be a significant differentiator. Certified organizations often experience a competitive edge with prospective clients and partners, due to improved operational efficiency and streamlined processes for demonstrating information assurances. The certification represents a commitment to excellence, and subsequently is an attractive proposition in creating new business opportunities and partnerships. Additionally, it can shorten sales cycles by proactively articulating mature security and compliance processes to Chief Information Officers (CIO), Chief Information Security Officers (CISO), and security operations teams.

HITRUST Inheritance: Partner-Driven Compliance

Participating in the **HITRUST Shared Responsibility and Inheritance Program** provides a significant advantage to achieving and maintaining your certification. Inheritance programs let your organization inherit certified controls from an authorized service provider, helping you expedite the HITRUST certification process, saving you time, reducing redundancy, and enhancing trust for your clients. HITRUST Inheritance allows for smarter and faster compliance, enhancing security measures without compromise.

HITRUST Industry Trends

The HITRUST certification market is experiencing significant growth and transformation, particularly within the healthcare industry. Healthcare organizations are increasingly turning to HITRUST certification to bolster their defense mechanisms and ensure compliance with stringent regulatory requirements.

HITRUST offers the only proven assurance mechanism against threats, with 99.4% of certified environments reporting no breaches in the last two years. It stands out as the sole assessment and certification system that provides validated, quantifiable assurance, demonstrating an organization's dedication to security. This highlights the trust and reliability organizations place in the HITRUST framework, which integrates insights from over 50 global standards to remain adaptive to emerging threats.

HITRUST-certified entities can demonstrate a strong commitment to addressing cybersecurity threats, due to continuous improvement and maturity of their information security management program. As a result, 92% of scoped controls that initially did not meet the HITRUST CSF framework are being remediated within one year of certification.

Low Breach Rate and Assurance

HITRUST's Cyber Threat Adaptive approach is central to maintaining relevance by regularly updating its control specifications based on threat intelligence and breach data. The Inaugural 2024 HITRUST Trust Report indicates a remarkable statistic: a notably low breach rate of 0.64% in certified environments over recent years. This low breach rate is a testament to the framework's robust security measures and its ability to significantly reduce cyber and information risk.

AI and Ransomware Threats

As AI technologies become more integrated into healthcare operations, HITRUST is proactively addressing the associated security concerns. The anticipated HITRUST AI Certification, expected in late 2024, will provide specific security controls for AI systems, equipping organizations to manage risks related to AI and ransomware threats effectively.

Regulatory Compliance and Cyber Insurance

HITRUST can play a crucial role in helping organizations navigate complex regulatory landscapes by aligning to one validated and recognized set of standards, designed specifically for healthcare organizations. By mapping to multiple authoritative sources such as HIPAA, GDPR, NIST, and ISO, HITRUST offers compliance solutions that are essential for healthcare providers managing sensitive data.

Additionally, HITRUST is influencing the cyber insurance industry. Insurers are increasingly looking for enhanced security assurances and metrics derived from frameworks like HITRUST to inform coverage decisions. Organizations with a HITRUST certification can experience more favorable cyber insurance options, as the certification exemplifies a high level of insurability due to third-party validated security preparedness and cyber resilience.

Assess Your Business

Do You Need HITRUST?

Consider the following questions as they relate to your business

Strategic Alignment with HITRUST Certification

- What are our current business goals and how does HITRUST certification align with them?
- Is HITRUST certification essential for winning larger or more strategic contracts with healthcare organizations, including hospitals, insurers, or government agencies?

Compliance & Regulatory Considerations

- Do we operate in a regulatory environment (e.g., HIPAA, HITECH Act) that necessitates comprehensive compliance frameworks like HITRUST?
- Would HITRUST certification help demonstrate compliance with multiple regulatory requirements, such as GDPR, CCPA, or other global privacy standards?
- What are the key compliance and security gaps in our current policies and procedures (if any) that HITRUST CSF alignment/certification could help address?

Risk Management & Cybersecurity Maturity

- How mature are our current cybersecurity policies and practices?
- What are the primary risks we face (e.g., data breaches, ransomware, compliance failures), and how will HITRUST help mitigate these?
- Do we have a strong incident response and breach notification process, and would HITRUST improve our current response capabilities?
- What is our current cybersecurity framework (e.g., NIST, ISO, SOC 2), and how will HITRUST complement or replace these frameworks?

Resource & Cost Considerations

- What are the estimated costs of obtaining and maintaining HITRUST certification (including assessment fees, audit costs, and internal resource allocation)?
- Do we have the internal resources (e.g., compliance officers, IT staff) to dedicate to the certification process, or would we need to hire or outsource expertise?
- Will HITRUST certification impact our overall IT and compliance budgets?

Customer & Partner Expectations

- What are the expectations of our healthcare customers in terms of compliance and data security certifications?
- Are our customers (especially in the healthcare industry) or partners demanding HITRUST certification as a requirement?
- Could HITRUST certification improve the trust and reputation we have with our customers, or is this more of a "nice to have"?
- Are any of our key partners or vendors already HITRUST certified, and if not, are they planning to be in the future?

Long-Term Benefits & Return on Investment

- What are the potential long-term business benefits of HITRUST certification, such as new revenue opportunities, improved customer trust, or reduced risk of regulatory fines?
- Could this certification help reduce insurance premiums or increase coverage limits related to cybersecurity insurance?

Evaluation of HITRUST Inheritance Program Partners

- Do we already have key vendors or partners who are part of the HITRUST Inheritance Program, and what controls can we inherit from them?
- Will inheriting controls from a vendor reduce our overall effort in achieving and maintaining HITRUST certification?
- Would working with an inheritance program partner help us reduce our costs and expedite the certification process?
- If considering a new vendor or partner, should their HITRUST certification status be a factor in our decision?

Operational & Technical Considerations

- Do our current systems and technical infrastructure align with HITRUST's control requirements?
- How will HITRUST certification impact our data management, cloud services, and third-party vendor management processes?
- Do we need to perform a gap analysis to understand where we currently stand in terms of meeting HITRUST requirements?

Cultural & Organizational Readiness

- Do we have executive buy-in and support from leadership for the investment and time required for certification?
- Is our organization culturally ready to adopt and maintain the rigorous processes required for HITRUST certification?

HITRUST Certification Preparation Checklist for Healthcare Companies

HITRUST

1. Conduct a Self-Assessment

- ☐ Use the MyCSF tool to evaluate current compliance status.
- ☐ Identify existing security controls and processes.
- ☐ Pinpoint areas needing improvement.
- ☐ Internally evaluate compliance with the HITRUST CSF controls, identifying areas needing improvement before a formal external review.

2. Identify Gaps

- ☐ Compare current practices against HITRUST requirements.
- ☐ Document all discrepancies and areas for enhancement.
- ☐ Evaluate whether your SecOps team has the capability to meet HITRUST requirements, or engage with a HITRUST-Certified partner through HITRUST Inheritance (see **6** below)

3. Allocate Resources

- ☐ Assign a dedicated team to manage HITRUST certification.
- ☐ Ensure budget allocation for necessary tools and personnel.
- ☐ Consider hiring external specialists if needed.

4. Train Staff

- ☐ Develop comprehensive training programs on HITRUST requirements.
- ☐ Conduct regular workshops and sessions to update staff on best practices.
- ☐ Foster a culture of compliance and security.

5. Implement Necessary Security Controls

- ☐ Integrate robust cybersecurity tools that align with HITRUST standards.
- ☐ Automate compliance monitoring and reporting processes.

6. Engage with HITRUST-Certified Partner

- ☐ Check the vendor's certification status on the HITRUST website or request their HITRUST CSF certification documentation directly.
- ☐ Utilize consultants for insights and assistance in addressing complex requirements.

7. Set Up Continuous Monitoring Systems

- ☐ Establish systems to track compliance metrics and performance indicators and schedule periodic internal audits to ensure ongoing adherence to HITRUST standards.

8. Prepare Documentation

- ☐ Gather and organize all necessary documentation for the HITRUST assessment.
- ☐ Ensure all policies, procedures, and reports are up-to-date and easily accessible.

9. Plan for Continuous Compliance

- ☐ Develop a strategy for maintaining compliance post-certification.
- ☐ Regularly review and update security measures as necessary.

Compliance Through Strategic Partnership

The Next Step to Achieving HITRUST Certification

Achieving HITRUST certification doesn't have to be a source of stress. By adopting a streamlined approach and partnering with the right experts, securing the certification sought by healthcare clients becomes possible, allowing a sharper focus on business initiatives.

ClearDATA is **HITRUST CSF r2 Certified** and is an authorized HITRUST Shared Responsibility and Inheritance Program provider. The program enables us to make our relevant assessment scores available for inheritance by participating organizations' completing their assessment. Through HITRUST's Inheritance program, customers have been able to inherit up to 85% of the controls* directly from ClearDATA.

**Exclusions apply depending on the scoped environment applicability to ClearDATA's inheritable controls.*

By partnering with ClearDATA, your business...

ClearDATA HITRUST Inheritance: The Benefits

- Simplifies the process and reduce the effort for hosting and service organization customers.
- Reduces the required testing and associated costs when inheriting technical controls.
- Reduces testing required when performing a HITRUST CSF Validated assessment.
- Reduces data entry and evidence requests associated with a Validated assessment of scoped requirements hosted in the HITRUST CSF Validated environment.
- Lets you inherit granular, detailed control requirement scores, not just broad categories.

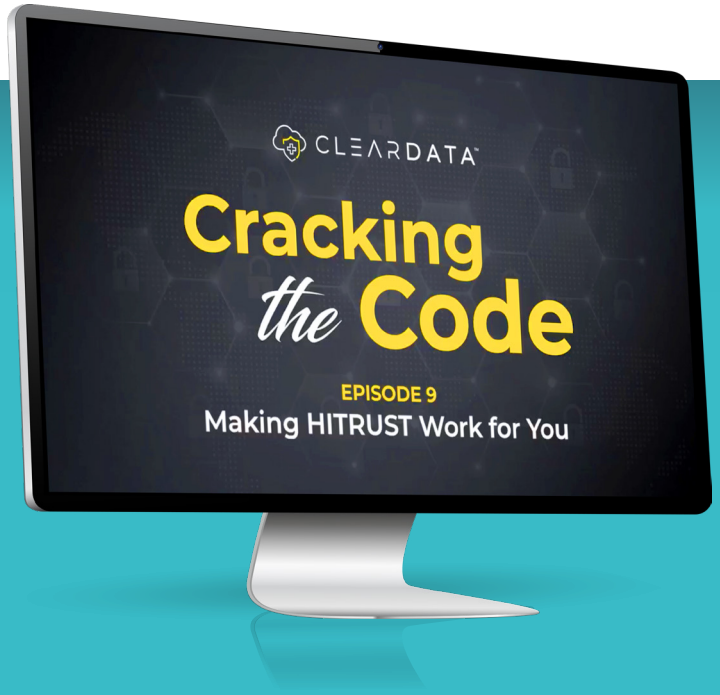
How does ClearDATA help you?

ClearDATA's CyberHealth™ Platform and managed services — Continuous Compliance, Cloud Operations, and Managed Detection and Response — together significantly alleviate the challenges customers face in implementing various technical control requirements, making security and compliance more manageable for the business. The platform offers comprehensive features that extends beyond those directly engaging in the Inheritance process.

At the heart of ClearDATA's offering are defined technical controls, each reinforced by numerous safeguards designed to evaluate, restrict, and remediate potential vulnerabilities, weaknesses, and compliance drift. Combined with managed services, this layered approach not only enhances security and compliance, but also streamlines cloud operations to help drive efficiency.

Customers benefit from ClearDATA's HITRUST r2 certification, regardless of whether they are actively pursuing their own certification while leveraging the Inheritance program, or simply managing their cloud workloads in conjunction with the CyberHealth Platform and managed services. Our commitment to data security and privacy, while ensuring regulatory compliance means customers can achieve a higher level of security, compliance, and ultimately, peace of mind.

ClearDATA empowers every customer, fostering a safer and more secure environment in the public cloud.



MACHINIFY

"The doors to many of our business opportunities wouldn't be open if we couldn't articulate a high level of certainty around security and compliance. We can demonstrate that certainty by running ClearDATA on AWS."

Watch Now

Advancing Healthcare with HITRUST

Achieving HITRUST certification is a strategic imperative for healthcare organizations striving to maintain the highest standards of data protection and managing cyber risk. Evaluating and implementing control requirements, remediation of gaps, continuous compliance, and regular assessments are fundamental steps for ensuring your organization is well-prepared to meet rigorous security and compliance standards.

Each HITRUST certification process requires resources that your team may lack. As technologies become increasingly sophisticated, and as HITRUST standards grow more rigorous, it presents an opportunity for organizations to consider partners with dedicated and strong cloud operations and security operations teams.

Partnering with an organization that serves as an extension of the organization's cloud and security operations teams can effectively address the challenges posed by talent shortages, lack of dedicated personnel, and tooling needs. This type of partnership alleviates increasing operational burdens and enhances the overall value of maintaining a comprehensive information security management program.

Ultimately, the path to successfully implementing HITRUST involves a holistic understanding of internal and external resources, paired with cutting-edge security solutions. By prioritizing these considerations, healthcare technology organizations can achieve not only compliance but also a sustainable security and compliance practices that support long-term operational trust and assurance in increasingly complex regulatory and threat landscapes.

95 CSAT Score

"Excellent!" ★★★★★

"ClearDATA makes it easy to use the same AWS services we're familiar with, but inside a HIPAA- and HITRUST-compliant environment."

...and so many more

Reach out today to schedule a consultation with one of our experts, who will help you find the best solution for your organization's healthcare cloud compliance and security needs.

ClearDATA.com (833) 99-CLEAR

Schedule a Consultation

CLEARDATA®