

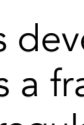
COMPLIANCE UNDER PRESSURE


Forming a Strong Cybersecurity Program Through HITRUST Certification


Healthcare organizations and vendors are increasingly under pressure to demonstrate compliance with cybersecurity and risk management leading practices and regulatory requirements. Pursuing alignment and certification with the HITRUST CSF has become one of the most effective ways of demonstrating strong healthcare cybersecurity program implementations.

This brief infographic can help answer some basic questions about HITRUST and HITRUST certification processes.

WHAT IS HITRUST?

 HITRUST is a non-profit organization that created and maintains the HITRUST CSF and HITRUST Assurance Program

 HITRUST was developed specifically for the healthcare industry and now provides a framework for organizations in every industry to comply with various regulations and standards based on the organization's size, types of systems deployed, and applicable regulatory requirements

 Meditology's CEO, Cliff Baker, served as the lead architect for HITRUST CSF, and Meditology has conducted hundreds of HITRUST assessments and certifications for healthcare entities

WHAT CERTIFICATION & ASSESSMENT OPTIONS DOES HITRUST OFFER?

HITRUST offers the following options:



HITRUST bC
Basic Current State Assessment




HITRUST i1
Implemented 1-Year Validated Assessment and Certification





HITRUST r2
Risk-based 2-Year Validated Assessment and certification

*The HITRUST r2, formerly called the CSF Validated Assessment, is the most adopted HITRUST certification.

The difference between these HITRUST assessments and certification options is the variance in level of effort and level of assurance that each assessment provides.

 **The HITRUST Basic Current State (bC) Assessment** provides a basic level of assurance and requires a review of only 71 security controls. The HITRUST bC assessment is not a certification; the bC is a verified self-assessment and does not require an external assessor firm to complete. Instead, it leverages the HITRUST Assurance Intelligence Engine to identify errors, omissions, or deceit, which is why HITRUST calls this a "Verified" Self-Assessment.




 **The HITRUST Implemented, 1-year (i1) Validated Assessment + Certification** delivers a relatively moderate level of assurance for information-sharing environments with lower risk thresholds. It is designed around relevant information security risks and emerging cyber threats and includes a combination of good security hygiene controls and best-practice controls. The HITRUST i1 maps and provides significant coverage around standards and authoritative sources generally viewed as security best practices, such as NIST SP 800-171, HIPAA Security Rule, GLBA Safeguards Rule, U.S. Department of Labor EBSA Cybersecurity Program Best Practices, Health Industry Cybersecurity Practices (HICP); as well as the HITRUST CSF framework requirements included in the HITRUST Basic, Current-state (bC) Assessment. The HITRUST i1 is good for one year and organizations are evaluated against the implementation of controls only. As a certifiable assessment, the HITRUST i1 requires an external assessor firm like Meditology Services to complete. The level of effort to achieve the HITRUST i1 certification is substantially less than the HITRUST r2 certification and is reportedly more on par with the level of effort for a SOC 2 Type II attestation.

 **The HITRUST Risk-based, 2-year (r2) Validated Assessment + Certification** provides a high level of assurance and is tailorable, requiring a minimum review of 198 controls (360 on average per assessment and 2000+ from which to choose, depending upon controls requirements) to obtain certification. The HITRUST r2 certification is valid for a two-year period with an interim review required at the one-year mark. Organizations are evaluated on security policies, procedures, implementation, measurement, and managed practices. The HITRUST r2 certification includes a comprehensive alignment with industry standards and regulatory requirements including the NIST Cybersecurity Framework and HIPAA (including the HIPAA Security Rule) among many others.

WHAT IS THE RELATIONSHIP BETWEEN HIPAA AND HITRUST?

- The HITRUST CSF gives organizations a way to show evidence of compliance with HIPAA-mandated security controls
- HITRUST takes the requirements of HIPAA and builds on them, incorporating them into a framework based on security and risk
- HITRUST certification provides prescriptive and measurable criteria and objectives for applying "appropriate administrative, technical, and physical safeguards" required by HIPAA
- HITRUST does not replace or substitute your HIPAA compliance program or "prove" that an entity is HIPAA compliant, but it is widely accepted as a best practice approach for healthcare entities to evaluate and manage risk in alignment with HIPAA requirements
- The U.S. President signed HR 7898 into law in January 2021, amending the HITECH Act to require HHS and OCR to recognize and promote best practice security for meeting HIPAA requirements. Specifically, the new law incentivizes covered entities and business associates to adopt industry best practices, including the HITRUST CSF

WHY GET HITRUST CERTIFIED?

-  Healthcare has become a prime target for malicious actors bent on profiting from the resale and reuse of patient information
-  Healthcare entities are scrambling to shore up security controls for their own organizations and third-party business partners as the sprawl of patient information continues to drive widespread data breach events
-  Many healthcare covered entities and business associates servicing the industry are pursuing or evaluating HITRUST certification to provide assurance of their security program and control effectiveness to the market

WHO NEEDS A HITRUST CERTIFICATION?

The most common organization types that pursue and obtain HITRUST certification include vendors and business associates servicing the healthcare industry, healthcare insurance and payors, and healthcare providers.

HOW LONG DOES IT TYPICALLY TAKE TO GET CERTIFIED?

<p>+6 MONTHS</p> <p>Very few, if any, organizations obtain certification earlier than 6 months into the process</p>	<p>9 MONTHS TO 1 YEAR</p> <p>The typical duration for a HITRUST certification process ranges from approximately 9 months to 1 year</p>	<p>+1 YEAR</p> <p>Many organizations take more than a year from start to finish to obtain formal certification status</p>
--	---	--

MEDITOLOGY: LEADERS IN HEALTHCARE CYBERSECURITY AND HITRUST SERVICES

Meditology is an authorized HITRUST external assessor organization and we have a dedicated team of HITRUST experts available to discuss your specific certification needs.

Contact us if you have any questions about healthcare security certification options and approaches.

"I rate the value of working with Meditology on our HITRUST Certification as "Exceptional" – 5 out of 5 rating. 2020 was a difficult year but we would not have gotten the results without working with Meditology as a partner because of the thoroughness, attention to quality, and stick-to-it-iveness. We have a legit HITRUST with no CAPs.

- AVP, Governance Risk & Compliance, National Direct Access Care Network and Wellness Organization

"Meditology saw us all the way through as they always have, we got our cert, they moved staff and timelines around, and they were very flexible in seeing us to the end. We were very happy with the deliverables. And A+ for getting us to the HITRUST Certification. We are satisfied, our Board and Execs are happy.

- Director of Security, Software Development Company

"I felt a strong sense of partnership right from the beginning. Meditology is competent and knowledgeable about who we are and how we are trying to achieve our HITRUST Certification goals, and that's a big part of success."

- CISO, One of the Nation's Largest Healthcare Payors