Med Tech Solutions

Cloud Confidence for Healthcare with HITRUST Common Security Framework (CSF)

The strongest security framework to protect critical healthcare data

With healthcare organizations facing escalating cyberattacks, one-time security assessment scores and snapshot certifications are no longer enough. The HITRUST Common Security Framework (CSF) provides an unmatched security foundation based on continuous assessment and controls.

WHAT YOU NEED TO KNOW TO SECURE YOUR PRACTICE

The costs of data ransom, regulatory fines, business disruption, and loss of patient trust have made security controls for critical healthcare data a top priority for IT professionals.

IT security and compliance regulations and best practices are defined by an array of federal and state regulations and industry standards, as well as policies and frameworks from a variety of associations and bodies. All that makes it difficult for provider organizations to fully understand what they need to do to mitigate security risk. For many organizations, an annual HIPAA assessment acts as the foundation for their security measures, but today's threat landscape is evolving in sophisticated ways every day.

And the stakes are high.

Without the proper systems in place, healthcare organizations may be exposed to security breaches or noncompliance with industry standards. Penalties can be directed at providers, the organization, and even individuals who have responsibility for the organization's security policies and practices. In addition, the impact of bad press and loss of patient trust may never be fully recoverable.

Unfortunately, many providers still struggle to create and maintain effective risk-mitigation policies and procedures. Demands for providers and staff to serve more patients often lead to security controls being softened for user convenience. For resource-constrained healthcare IT departments, an additional challenge is to understand the requirements and implement them with an IT strategy that is also affordable, manageable, and scalable over time.

Cloud hosting that is HITRUST CSF-certified is one of the most strategic and effective ways for healthcare organizations to gain confidence in their IT security posture. By including federal and state regulations, standards, and frameworks, and incorporating a risk-based approach, the HITRUST Common Security Framework (CSF) helps organizations address risk through a comprehensive and flexible framework of prescriptive and scalable security controls.

Cloud hosting that is HITRUST CSF-certified is one of the most strategic and effective ways for healthcare organizations to gain confidence in their IT security posture.

Where HIPAA, HITECH, and HITRUST Overlap

The Health Insurance Portability and Accountability Act (HIPAA) defines standards for organizations to safeguard patient data, and repercussions if those organizations fail to do so. Healthcare organizations and business associates must implement and prove—through annual HIPAA audits and assessments—that they have put safeguards in place to protect patients' personal health information (PHI).

The Health Information Technology for Economic and Clinical Health (HITECH) Act expanded the scope of privacy and security protections within HIPAA compliance. HITECH introduced different methods of audit and assessment and increased fines, motivating organizations to take security and compliance seriously.

But over more than two decades of existence, HIPAA has become complicated by interpretations, state and local protections, and health IT advances that lawmakers are struggling to keep up with. The result is that for most provider organizations, simply meeting HIPAA requirements is not enough to keep data secure.

That's where HITRUST comes in.

HIPAA ENFORCEMENT UPDATES TIMELINE

1996

HIPAA ENACTED

$100 CMP per violation with $25K annual limit

2003

INTERIM RULE

Interim rule issued; 2005 enforcement provisions proposed

2006

HIPAA ENFORCEMENT RULE

Penalties still $100 per violation and $25K annual limit

2009

HITECH ACT

4-tier culpability model; $1.5M annual limit for all tiers for identical violations

2019

NEW CMP ANNUAL LIMITS

$25K limit for tier 1
$100K limit for tier 2
$250K limit for tier 3

HITRUST AND THE COMMON SECURITY FRAMEWORK (CSF)

While HIPAA is an act that details standards for compliance, HITRUST is an organization that specifies rigorous security requirements and controls used to measure an organization's ability to safeguard PHI.

HITRUST INTEGRATES 40+ GLOBAL SECURITY STANDARDS

HITRUST is one of the most widely adopted security frameworks, covering more than 40 authoritative sources including these global standards:

- HIPAA
- National Institute of Standards and Technology (NIST)
- International Organization for Standardization (ISO)
- Payment Card Industry (PCI)
- Federal Trade Commission (FTC) Red Flag
- Control Objectives for Information and Related Technology (COBIT)

The HITRUST organization helps organizations address the complexities and achieve compliance with HIPAA regulations using the HITRUST Common Security Framework (CSF). HITRUST CSF is used to measure the requirements of the HIPAA Security Rule along with other relevant and comprehensive global standards, regulations, and frameworks to provide a clear and prescriptive set of controls for achieving HIPAA compliance. There are currently more than 400 HITRUST controls and implementation requirements, making this certification a significant commitment. This is far more stringent than typical audits such as SSAE 18 and SOC 2 that are often touted by datacenters, but which simply demonstrate snapshot compliance to physical and logical controls.

The HITRUST CSF has become the definitive information-protection framework for the healthcare industry. It is the industry gold standard and the benchmark against which organizations measure themselves when charged with safeguarding PHI. HITRUST certification attests that an organization has met the relevant requirements within the CSF framework. Certification of controls testing by a third party gives vendors a common benchmark of multiple relevant standards to meet the requirements for every client organization.

MTSCloud is a HITRUST CSF-certified platform

The Med Tech Solutions (MTS) private cloud platform has achieved HITRUST CSF certification since 2019. This demonstrates that MTS has met key information-protection requirements related to how information is accessed and stored in its cloud environment. Certification places us in an elite group of organizations worldwide who have worked to meet this rigorous security framework.

The MTS Cloud HITRUST CSF-certified platform helps organizations manage risk, improve security posture, and meet compliance requirements. This commitment helps our clients set high standards in protecting patient and business data. HITRUST, which pulls from numerous regulatory frameworks including NIST, HIPAA, and ISO 27001, has become the gold standard in protecting healthcare information.

For healthcare practices—as well as organizations who provide IT services to support those practices—a cloud hosting partner that is HITRUST CSF certified gives immediate peace of mind. and saves these organizations from conducting time-consuming vendor compliance audits. Knowing that the vendor follows the HITRUST CSF framework provides a level of assurance that ePHI is handled in a consistent manner. This, in turn, saves time and results in better synergies.

In addition to implementing the controls required for our private cloud infrastructure, we also apply the extensive learnings from the process of HITRUST certification to every aspect of our business. We are a security-first cloud and IT services provider, with an ongoing mission to protect our clients' critical data and their ability to serve patients.

Talk to us about moving your critical patient and practice applications to the MTSCloud.

> "Security is a big concern for all organizations, especially when you're dealing with personal health information. The HITRUST certification that MTS was able to provide made the security analysis and risk assessment that we have in place very easy. It gives me the confidence knowing that we have the best security in place to be able to give the providers and the patients peace of mind, knowing that their data is protected in that hosted environment."
>
> — Armando Besné,
> senior manager of CIS at MTS client OptumCare

"The fact that Med Tech Solutions has achieved HITRUST CSF Certification attests to the high quality of their information risk management and compliance program."

HITRUST CSF Certified

BIMAI SHETH,
VICE PRESIDENT OF ASSURANCE SERVICES,
HITRUST

Learn how our HITRUST-certified cloud hosting can improve your organization's privacy and security stance. Contact us at info@medtechsolutions.com

Med Tech Solutions

medtechsolutions.com | 877.687.1222

Med Tech Solutions (MTS) creates technology systems that work the way healthcare practices work. Our Practice-Centered Care services use dedicated IT Care Teams to ensure that technology systems support essential clinical workflows. Provider organizations and networks get a secure, reliable IT infrastructure, optimized clinical and business applications, and full end-user support so they can focus on patient care. MTS was founded in 2006 and is headquartered in Valencia, California. The company has been recognized as an Inc. 5000 Fastest-Growing Company and a Channel Futures MSP 501 provider, and has achieved HITRUST Common Security Framework (CSF) certification for its cloud platform. Learn more at medtechsolutions.com.

6 BEST PRACTICES

Cybersecurity in Healthcare Checklist

Healthcare remains a primary target for cybercrime. It's not a matter of *if* you'll be attacked, but *when*, so the best approach to security is a proactive one.

Traditional security tools used over the last 15 years such as signature-based antivirus and perimeter firewalls are ineffective in dealing with multi-faceted advanced persistent threat (APT) campaigns. The APT's objective is to evade defenses and gather as much information about the environment as possible, allowing threat actors to maximize their impact.

6 THINGS HEALTHCARE ORGANIZATIONS CAN DO TO PROTECT THEMSELVES

1. Many breaches occur on desktops, laptops, and mobile devices, so using **endpoint detection and response (EDR) technologies** protects the endpoint before the breach occurs. EDR works in conjunction with security information and event management (SIEM) technologies that analyze, detect, and alert IT departments about potential threats. These tools must be managed by a 24×7 security operations center and a qualified 24×7 incident response team to detect lateral movement and ensure anomalies on the network are found and stopped as quickly as possible.

2. Use the **principal of least privilege for user access** as well as administrative access. This minimizes the number of users with elevated privileges, which also minimizes the number of potential APT targets, making it more difficult for threat actors to gain elevated access to an environment.

3. Apply **traffic monitoring tools** to detect any suspicious flows or anomalies. Monitoring and detecting suspicious flows prevents exfiltration or data loss before it occurs.

4. Utilize **multi-factor authentication (MFA)** to make it difficult for hackers and threat actors to compromise a system. Even if they obtain or guess a password, MFA adds another layer of protection to prevent an account from becoming compromised. Using MFA can also help you meet industry compliance requirements such as HIPAA.

5. Ensure **up-to-date security patching**. This foundational security practice ensures all systems have software vendors' latest security patches. A vigilant approach to patching minimizes the chances of an APT exploiting vulnerabilities in operating systems and applications.

6. Conduct regular **security awareness training (SAT)** to keep security at the top of mind for employees so they don't easily fall prey to targeted phishing campaigns or social engineering. It is one of the easiest steps any organization can take to protect themselves from APT attacks.

Finally, if an incident occurs – when every second counts to limit damage and restore vital services – it is critical to have an incident response plan in place.

Many victims of cybercrime are left scrambling to figure out what to do when they find ransomware or discover their data has been compromised. If that is the first time your security vendors interact, that can cause expensive delays and additional losses.

The best approach to security is a proactive one. That's why Med Tech Solutions offers a comprehensive security platform that protects and prepares your organization, giving you—and your patients—confidence and peace of mind.

Med Tech Solutions

medtechsolutions.com

Let Med Tech Solutions help you develop a holistic plan to fortify your overall security posture.

CONTACT US FOR MORE INFORMATION AT 877-687-1222 OR INFO@MEDTECHSOLUTIONS.COM