

Helping Medical Device Manufacturer Achieve HITRUST™ Certification

As the frequency and sophistication of cyberattacks continue to escalate, it's more important than ever to identify partners that can help fortify your defenses. This is especially true in the medical device environment, where cyberattacks can compromise highly sensitive patient data or even threaten patient health.

This case study describes how Tevora helped an industry-leading medical device manufacturer prepare for and achieve HITRUST Common Security Framework™ (CSF) Certification. Achieving this certification has added a valuable tool to the manufacturer's sales arsenal because it demonstrates to their clients that they are well-defended against cyberattacks and compliant with HIPAA, Omnibus, and other applicable federal and state requirements.

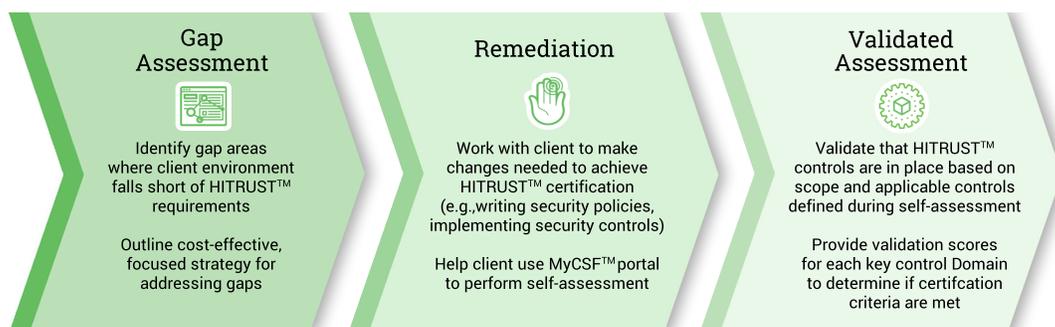
To protect our client's confidentiality, we'll refer to them by the fictitious name of Medical Devices International (MDI).

Partnering with MDI to Achieve HITRUST CSF™ Certification

As a certified HITRUST™ Assessor, Tevora was able to help MDI prepare for HITRUST CSF™ Certification and conduct a formal assessment to validate their compliance.

We've honed our certification methodology as we've helped some of the world's largest medical device manufacturers reach this significant milestone. Here's a summary of the methodology:

Tevora's Proven HITRUST™ Methodology



We followed this general methodology to help MDI prepare for and achieve HITRUST™ certification, but as with every engagement, there were unique challenges associated with this project.

In some cases, we've been called in to help a client achieve HITRUST™ certification for a specific application or device. In the MDI case, we helped them certify their entire environment, including multiple applications, platforms, internal networks, and medical devices.

Another complex aspect of this project was that some of the medical devices requiring certification were deployed in MDI client environments at hospitals where they were used to make video recordings of surgeries, then sync the videos to the cloud where they could be used for training and education purposes. This required relatively complex controls to ensure the security of these remotely deployed devices and their communication with cloud applications.

Tevora worked side by side with MDI to help them design feasible and realistic controls that would address the specific requirements of HITRUST™ and enable them to achieve the passing scores needed in each Domain for certification. We used a highly collaborative approach, running many iterations of different techniques and tools until we concluded that the HITRUST™ requirements had been met. We needed to roll up our sleeves and get down into the detail to help them design and implement the necessary controls—just the kind of work we love!

Another challenging aspect of this project was helping our client team to navigate the complicated, and sometimes convoluted, internal corporate processes needed to gain approval for and implement the required controls. Fortunately, our experience with other large, complex clients enabled us to add significant value in this area.

Thanks to the strong working relationship we established with the MDI team, and our deep security expertise and knowledge of HITRUST™ requirements, we were able to complete the certification ahead of schedule, while ensuring a high level of security for MDI.

In addition to increasing confidence in the security of their systems, MDI has been pleasantly surprised to find that their HITRUST™ certification status is an invaluable tool for their sales efforts.

“The significance of a HITRUST certification for healthcare organizations moves beyond the realm of security and compliance,” said Marc Sabelli, Tevora’s Healthcare Account Director, who worked closely with MDI on the certification process. “For an organization, be it medical device or other, HITRUST certification symbolizes an increased commitment to patient care that extends to every aspect of the business.”

Certification shows that the priority of the business is to deliver highly secure patient care at every level and to provide the utmost protection of the patient’s data, which results in efficient and effective treatment. HITRUST builds confidence within the healthcare industry that a patient’s information and treatment plan can be trusted with the certified healthcare organization.



HITRUST™ Overview



Founded in 2007, HITRUST™ offers the only universally-recognized healthcare information security certification.

It is governed by a Board of Directors composed of healthcare industry leaders. The HITRUST CSF™ addresses the multitude of security, privacy, and regulatory challenges facing healthcare organizations today. With a comprehensive yet flexible framework of prescriptive and scalable security solutions, it incorporates a risk-based approach to compliance with federal and state regulations—and common standards and frameworks—to help organizations address these challenges.

HITRUST™ offers an online “MyCSF™” web application that is used to facilitate HITRUST CSF™ self-assessments (gap assessment) and HITRUST CSF™ validated assessments (audit for certification). Both the HITRUST™ Approved Assessor and the entity being assessed are required to interact with MyCSF™, which streamlines the certification process.

HITRUST™ audits the auditor on 100% of assessments, ensuring ongoing integrity and quality of HITRUST™ Approved Assessors.

There are 19 Domains covered in HITRUST™ certification (e.g., Information Protection Program, Endpoint Protection, Portable Media Security). Each Domain has multiple requirements that are individually scored. To achieve compliance, an organization must achieve a composite score of at least 62% for each Domain.

HITRUST™ Benefits

Organizations achieving HITRUST CSF™ Certification will realize significant benefits, including:



Confidence that you have a high level of security in your healthcare systems and network environment and are well-defended against cyberattacks



Assurance that your organization is compliant with the complex and varied set of applicable government and industry requirements, including HIPAA, Omnibus, and other relevant federal and state requirements



Excellent tool for demonstrating to clients that your organization is committed to security and that their valuable data is safe and secure

Let Tevora be Your Trusted Partner

Tevora's expert team of security specialists can partner with you to help build up your defenses against ransomware and other cyberattacks. This includes reviewing your environment for potential security weaknesses, implementing tools and techniques to protect your environment, and training your staff to be aware of emerging ransomware, phishing, spearphishing, and social engineering trends, so they are fully equipped to be the first line of defense against attack.

If you do suffer a ransomware or other type of cyberattack, Tevora's experienced incident response team can jump in at a moment's notice to help you get back up and running quickly, while minimizing financial, operational, and reputational damage.

If you'd like to learn more about how Tevora can be your trusted security partner, just give us a call at **(833) 292-1609** or email us at sales@tevora.com.