SENSATO

Medical Device Cybersecurity Field Manual

A realistic guide to the design, development, and deployment of holistic medical device cybersecurity programs for healthcare organizations

LEARN MORE

✉ info@sensato.co

☎ 844.736.7286

🌐 www.sensato.co

Contents

Introduction

Several years ago, over a few cold and blustery days in March, the U.S. Food & Drug Administration ("FDA") held a cross-industry workshop to gather insights into the state of medical device cybersecurity. The workshop's turnout was strong, with representatives from the government, medical device manufacturing, hospitals, cybersecurity researchers, consultancies, and other cybersecurity and healthcare industry leaders. One thing that became clear, I suspect to all in attendance, was that we did not have a practical and realistic approach to medical device cybersecurity as an industry.

An outcome of the workshop, at least for me, was a personal calling to try and make a difference. Shortly after that, I founded the Medical Device Cybersecurity Task Force, or what would come to be known as the MDCTF. The MDCTF was an open-source group chartered to develop tactical practices and procedures for safeguarding medical devices and their supporting infrastructure. Ultimately, the objective was to quickly get something in place and leave the long-term medical device cybersecurity strategy to those with more patience, time, and resources.

The MDCTF grew to 83 members, a ragtag mix of hospitals, device manufacturers, government, consultants, and cybersecurity researchers. The group would alternate meeting in-person and virtually over two years. With time, the group's impact was recognized by the FDA. The MDCTF became an Information Sharing & Analysis Organization under the U.S Department of Homeland Security and today is known as the Sensato ISAO. More importantly, the Sensato ISAO, FDA, and H-ISAC entered a trilateral Memorandum of Understanding ("MOU") to share threat intelligence related to medical devices and formulate best practices in defending them from cyber-attacks.

Although there has been a tremendous effort to develop best practices and strategies for securing medical devices, the industry has not changed much since the formation of the MDCTF. That said, the need for securing medical devices has evolved with several incidents occurring that have demonstrated the need for a set of realistic and practical approaches for achieving medical device security.

Enter the Medical Device Cybersecurity Field Manual.

This manual aims to help you develop a holistic medical device cybersecurity program from nothing. The manual does not assume you have anything in place or have any medical device background or IT cybersecurity background.

Sensato started in 2013 as the first healthcare-specific cybersecurity firm. In 2015, before the FDA Workshop, we began to perform medical device cybersecurity risk assessments and, in 2018, were named the Medical Device Cybersecurity Firm to watch. Since 2015 we have responded to various medical device cybersecurity incidents and partnered with the FDA and the DHS to evaluate and respond to healthcare sector threats involving medical devices. We have performed ongoing research into medical device cybersecurity and provided tabletop simulations to over 150 healthcare organizations, with medical device cybersecurity being a cornerstone of those simulations. We have also worked closely with manufacturers to design, develop and deploy more secure medical devices.

We recently became the first company to design and develop a holistic medical device cybersecurity solution that meets or exceeds the FDA/MITRE recommendations for medical device cybersecurity preparedness and response, first published in October 2018. Our medical device solution is known as MD-COP. Although you will learn more about that solution, this manual's core focus is on designing and developing your own medical device cybersecurity program.

Ultimately, everything that our team and I have learned about medical device cybersecurity to date is included in this manual. Some may wonder why a cybersecurity vendor would share the secret sauce of their solution with the world, and to be clear, yes, there is a concern that our competitors will rob us of our jewels. However, we are willing to take that chance since we believe there is too much at stake in medical device cybersecurity to worry about trade secrets and competition.

As you read through the manual, you will find a variety of guidance and tools. We have tried to develop the manual as a blueprint. Although you can skip to any section and derive what you need, the manual will take you from ground zero to a successful deployment of a fully integrated and holistic medical device cybersecurity program. We also tried to make this a fun and easy read, so you will find the writing style casual, emphasizing usability instead of academia.

I hope you find the information within a practical and valuable addition to your journey. If you have questions, thoughts, or ideas, please feel free to reach out to me at john.gomez@sensato.co.

Respectfully,

John Gomez, CEO/Founder
Sensato Cybersecurity Solutions
www.sensato.co
844.736.7286

Medical Device Cybersecurity Not IT Cybersecurity

One of the critical challenges often seen is applying IT cybersecurity policies and procedures to medical device cybersecurity. Although some of the approaches to safeguarding IT systems can be recycled and used on medical devices, it is essential to keep in mind that medical device cybersecurity is a separate and distinct practice in cybersecurity.

IT cybersecurity is and has been focused on protecting systems and the data within those systems. Even HIPAA focuses on the protection of data. At first, this may sound as if it would be a practical approach for safeguarding medical devices. After all, IT systems and medical devices both have computer chips. They often use the same methods of communicating with the network, and yes, it is vital to safeguard the data on those devices. Since medical devices often contain and rely upon Protected Health Information (PHI) and Personally Identifiable Information (PII), they are regulated under HIPAA, in addition to their FDA requirements.

However, the critical difference is that medical devices have one thing that classical IT systems do not; A human is possibly relying on that computer to keep them alive. This may seem as if I am stating the obvious, but as obvious as that may seem, it is one of the most significant factors for designing, developing, and deploying a medical device cybersecurity program.

If you take frameworks like NIST CSF, NIST 800-53, or HIPAA and apply them to medical device cybersecurity, you may find that you achieve one thing; a false sense of security and readiness. Most IT cybersecurity practices fall short of what is required to support a medical device cybersecurity program.

This fact does not mean that some IT cybersecurity approaches would not work in medical device cybersecurity. Instead, you need to purposefully consider the differences and clearly understand where things may fall short. Let us take the example of cybersecurity incident response.

When you consider incident response from the IT perspective, the focus is on protecting systems and confidentiality, integrity, and availability of data. Protecting medical devices requires focusing on utilizing tools, tactics, policies, and procedures. This strategy is not a condemnation of those approaches; it is critical to the organization's success. But even though some ofthe IT cybersecurity incident response procedures may be a good start for medical device cybersecurity, they fall short when responding to medical device cybersecurity incidents.

In past conversations with people on this need to mentally shift our approach, some will point out that IT systems currently protect life. For example, it could be disastrous if an attacker were to modify order sets or allergy data in an EHR. So yes, the consequence to human life is real for non-medical device cybersecurity systems. That said, I would still maintain that as an industry, we fall very short when it comes to the deployment of tactics, techniques, and procedures that are organically designed to safeguard human life. As the industry matured, we inherited our cybersecurity best practices from sectors not focused on protecting human life. Much of what we inherited came from the financial sector. Even today, you will hear those walking the halls of a hospital speak about how we should learn from the financial industry regarding cybersecurity. If that is wise or not is beyond this manual's scope; it is essential to recognize that medical device cybersecurity requires different approaches than what we have classically embraced.

One of the foundational items needed to be successful in launching or evolving your medical device cybersecurity program is to get all stakeholders to agree that medical device cybersecurity is a new field and should be approached differently than IT cybersecurity. The impact on human life if an attacker is successful could be critical.

Another way to think of this is to reverse engineer the problem. Rather than start with "how do you protect" medical devices, you should start with how to protect the patient.

Things-to-Know/Consider

Medical Device Cybersecurity Focus- As you evolve your medical device cybersecurity, be careful not to simply inherit IT security best practices or approaches.

IT Security Focus – IT Security has traditionally focused on protecting systems and data, not patients. This is an important distinction and something you need to consider.

Staffing and Resources – Do you have the right people and expertise to help you design a medical device cybersecurity program?

Start with the Patient

Software Solves Everything!

If you listen to vendors or even cybersecurity professionals' recommendations, you will often hear how the right software is the cornerstone to an effective medical device cybersecurity program. Nothing could be further from the truth.

Sensato is a software company and provides some of the most robust cybersecurity software available; software that is beyond capable when it comes to supporting a medical device cybersecurity program. The keyword there is supporting.

The cornerstone of any medical device cybersecurity program should be the patient, not the software. Yes, the software is an essential component, but it is not the only component.
By starting with the patient, you uncover a series of questions, challenges, and needs that will help you formulate a much more in-depth strategy and approach. Many organizations that start with the software are usually responding to a vendor presentation and become what I call software focused. Unfortunately, once the software deployment is complete, they realize that there are many things the software does not address. Yet, when presenting the medical device cybersecurity strategy to leadership, no one highlighted that the overall investment to run a successful medical device cybersecurity program would be much higher. The software was just a small component.

The critical takeaway—do not fall into the trap that software is the crown jewel of your program. Yes, the software is needed, and there is a lot to consider when it comes to that decision. Still, suppose you put the software first. In that case, you may very well find that your overall costs will be much more significant than you expected and that depending on your approach, you may need to start over – including displacing the software you deployed.

Step back and consider all the components needed to support patient care before you start speaking to software vendors. This approach may not be comfortable for you or your IT cybersecurity team because we are more comfortable talking tech and safeguarding the device and data (seethe previous section). Yet, if we step back for a moment and consider the attacker's perspective, we may seethings a little differently.

The Attackers Perspective

A critical thing to keep in mind is that attackers will always have a vote. Some may even say that the attacker gets to choose all the options. They get to choose the type of attack, the time and date of the attack,the attack's ultimate objective, and how long and how many attacks to perform. Interestingly, many of our approaches to cybersecurity are often based on the defender's perspective. We tend to minimize the attacker’s skillset, tenacity, and audacity.

When it comes to medical device cybersecurity, we can represent the attacker's perspective by starting with the patient. To do that, we need to ask, "what could an attacker do to this patient if they were to compromise this medical device in some way, shape, or form?" In doing this, we not only give the attacker a voice, but we also begin to define the types of incidents we need to plan for, respond to, manage, and ultimately recover from as part of a medical device cybersecurity program.

There are a few different ways to do this, and it comes down to the number of staffed resources and timeline. You could undoubtedly review each medical device category and determine the type of attack, for example, smart pump versus MRI. Another approach would be to consider attacks against diagnostic systems versus life support systems. Approaching the broader categorization problem is faster and allows for broader conversation with your peers and colleagues. It also can help you refine needs in terms of compliance, detection, and response.

For example, you could build a matrix that identifies what you want to consider or require for each device category. You may decide that diagnostic devices' security assessment level is not as detailed as for life support devices. Your response to diagnostic devices may be different than for life support devices. The keyis to purposefully think about how these categories of devices shape your medical device cybersecurity program. It can also help you in terms of planning. For instance, if you have limited funds or resources, you may propose that you develop a multi-phase approach that starts by safeguarding and segregating life supportdevices as an organization. A separate phase would later focus on diagnostic devices.

All these considerations start with the patient and consider the attacker's perspective. We must continually step back and ascertain the impact on patient safety and the attacker's potential for harm. If we can maintain these approaches as the guiding principles, we can also lay the foundation for a defensible program. A defensible program is one in which we could support a robust legal defense. Please keep in mind that this manual, Sensato or I personally am not an attorney, and as you develop your medical device cybersecurity program, you should consult your legal counsel. By laying the foundation that your program focuses on patient safety and not only protecting systems and data, you are defining a strong future defense.

As we continue to think about the patient and the attacker, we find that much of what we believe is sufficient for medical device cybersecurity is false. We start to understand that many of the points already raised start to come to light. For example, we realize that there is much more to medical device cybersecurity than just deploying software. We need to consider the legal ramifications of our program's design, the need to evaluate our inventory and classify devices, the need to consider other strategies such as network segmentation and assess the device and manufacturer from a risk perspective. Within this manual, we will help you devise a plan to address all those decisions and challenges, but we need to go back to the patient and think about ***incident response*** before we do.

Things-to-Know/Consider

Attackers Get a Vote – You should always keep in mind that the attacker gets to decide the how, when, why and much more – if your cybersecurity strategy does not take this into account; you will achieve a false sense of security.

Start with the Patient - By always starting with the patient and asking "what could an attacker do to this patient when connected to a device" we are able to think of defenses and strategies that are specific, and patient centered.

Remember Defensibility – As you design your medical device cybersecurity program, you need to keep liability in mind. Always consult your legal counsel.

Incident Response Considerations

Cybersecurity incident response is often a somewhat misunderstood concept. In the over 150 tabletop simulations conducted, we have seen very few organizations perform well to a fast-moving realistic attack. There are reasons for this, including that much of what we do about cybersecurity is still back in 2010. Now keep in mind that we have very few well-known practices or guidance regarding responding to a medical device cybersecurity attack.

Getting medical device cybersecurity incident response right is critical. Before we jump into it, let's walk through a mini-tabletop simulation. This simulation should apply to any hospital, and it works best if you play along. After the simulation, I will walk through what was expected and provide suggestions for designing your medical device cybersecurity program.

As this simulation unfolds, think about how you would handle this based on the time of day, day of the week, level of training, and procedures deployed. Think about how well your IT cybersecurity policies and procedures would work. This simulation is a light version of our program. However, it is based on a real incident that the team responded to in 2019.

03:00 Sunday

An alert is raised by your cybersecurity software involving a patient monitoring system. The alert is related to a possible SSH Brute Force attack against Port 23 of a server on your network.

03:04 Sunday

An alert is raised that a client IP address is performing port and address scans of network assets.

03:05 Sunday

An alert is raised that a client IP address is attempting to utilize SMB to query network assets.

03:07 Sunday

Nurses in the ICU observe that their desktop computers used for patient monitoring have locked up and do not seem to work.

03:08 Sunday

Nurses in the ICU report that several medical devices seem to be acting "weird" and are concerned about their stability.

This scenario could continue to evolve, but we will use these events to illustrate a few points for our needs in this manual. The intent is to help introduce concepts to consider as we continue designing and developing your medical device cybersecurity program.

Before we dive into recommendations and practices, you should take a few minutes to think about all we have discussed so far. Everything we have reviewed comes down to how well you can detect, analyze, and respond to an attack. But while software supports it, this is not something done by software alone.

The incident described is about the impact on patients, which needs to be our core focus. This incident represents an active attacker in your environment who appears to be targeting medical devices at 3 PM on a Sunday. You can use this snippet of a simulation to add another test to your design – "what if this happened at 3 AM on a Sunday?" We call that the 3 AM test, and we use it because we find that most cybersecurity strategies are designed to work at 10 AM on Monday; a time when there are plenty of on-the-ground resources, a full complement of leaders, easy access to clinical engineering and third parties. But, at 3 AM on Sunday, you are short-staffed or not staffed, and suddenly things begin to fall apart. By considering the 3 AM Test, you can assure practices, policies, and procedures will survive regardless of the time of day or day of the week.

Continuous Monitoring

We just explained the 3 AM test, and as you probably agree, it is an important consideration. You can deploy excellent world-class software, but what good is it if an alert occurs at 3 AM on a Sunday and no one sees it until 9:30 AM the next morning? How you will monitor your system 24x7 is a critical item to keep in mind. Medical devices are not just 9-to-5 assets, and patients do not only need care during the day. Yet many IT Security teams are not 24x7, and even those with after-hours support may rely on a helpdesk or text messages to deal with critical events. It is one thing to deal with a crucial alert at 3 AM for a server and yet another to deal with a medical device attack.

Even if you have a 24x7 operation monitoring your alerts, you also need to consider their training. Do they have the appropriate knowledge to provide overwatch to a medical device attack? Most IT incident response focuses on determining what is occurring to the device or network, whereas medical device incident response needs to determine the patient impact; ideally, you can do both simultaneously.

Anomaly Awareness

In the scenario we outlined, the nursing staff observes strange behavior. In this case, we have the alerts' context. Still, in some situations, you may only have on-the-ground observations of anomalies, which means that we must address our clinical end-users training and the clinical engineering team to evaluate device behavior in the context of cybersecurity. Providing specialized security awareness training must be performed as the threat landscape evolves and incorporates comprehensive nursing education and management. Further, the helpdesk should also analyze reports of anomalies in the context of cybersecurity to support early detection of zero-day events or other events that do not raise system alerts.

Clinical Cybersecurity Rapid Response

A concept that Sensato pioneered in 2018 is known as Clinical Cybersecurity Rapid Response. In the scenario above, the attack targeted systems in the ICU, but this could easily have been the Cath-Lab, Surgical Suites, PACI, or similar highly critical hospital areas. In all these areas, we have life support systems that support patient care. The need to evaluate the threat is not something the IT Security teamcan do solely by themselves. The evaluation of the threat, the on-the-ground response, and patient careimpact must all be carried out in parallel as time is of the essence.

To accomplish this process, your clinical Rapid Response team must be trained to support cybersecurity issues. It would be best if you also considered that the Rapid Response team is limited in resources and that a cybersecurity attack can simultaneously impact many patients. Ultimately you need to design training and scenarios for these teams that remain current over time.

The Monitoring Dilemma

One item not illustrated in the above scenario is an attack that breaches a third-party medical device network. These networks are deployed and maintained by the vendor. We know that you cannot deploy monitoring tools (hardware or software) to these networks in all cases. Doing so may very well violate warranties and, in some cases, possibly put patient safety at risk. It is also possible that any cybersecurity device deployed to these networks would need to be cleared by the FDA.

This requirement creates a monitoring dilemma. Your software solution (remember, do not start with the software) may not identify attacks for those devices on these third-party networks. You should ascertain the warranty and patient safety implications of monitoring these devices.

Fingerprinting & Location

In the scenario, we provided details about what types of devices were involved and their location. But what if we did not provide those details? If your teams cannot identify the type of device (at the very least the manufacturer) and the device's location, how do you dispatch your rapid response team to determine patient state and impact? It is essential to decide on the location and type of device to supportincident response and support threat intelligence and vulnerability assessment activities. Major software vendors in this space support these features to varying degrees.

14-Minute Window

Years ago, we implemented what is known as the "14-minute window," which is simple— you need to detect, analyze, and successfully contain an attack within 14 minutes. This method is not something that a traditional IT Security approach typically will address. But when we start with patients, we know time is of the essence. We need to move quickly but with professionalism and context. As you design your program, consider what you could do in 14 minutes, and then if you achieve that, keep getting better by optimizing your response.

Protocols vs. Playbooks

Playbooks are an interesting approach to cybersecurity incident response. They are rather fine pieces of documentation that make for a great reference resource. Interestingly, when we conduct tabletop simulations, the first victim is the playbook. Teams bring their playbooks, but all references to the playbook are soon put aside after about five minutes.

The reasons for this are varied, but what we can gather is a matter of complexity. When an incident is evolving quickly, and you have less than 14-minutes to respond at 3 AM on Sunday, the last thing you will do is open a playbook. Our suggestion is to adopt a protocol-based incident response for medical device cybersecurity.

The goal of protocol-based incident response is to simplify the response and ultimately drive muscle memory. This approach is familiar for clinicians and was adopted from the Maryland Shock Trauma center back in 2014. As you consider how you will train your teams to respond in a coordinated fashion to medical device cybersecurity incidents, you should consider developing protocols instead of playbooks.

Comply – Detect – Respond

The first part of this manual focused on providing a practical set of knowledge and considerations that you can use to help lay the foundation for the design, development, and deployment of a medical device cybersecurity program. As you now know, we recommend that you start by thinking of the patient first, keep the attacker's perspective in mind and consider how you prepare well for a real-world attack.

In this next section, the approach changes to be more prescriptive, providing a series of questions to consider, with recommendations, that you can use in formulating your medical device cybersecurity program. The questions are not a complete representation of all considerations, but hopefully, it provides a strong foundation. More importantly, I hope that these items help you become more familiar with a medical device cybersecurity program's various components.

The recommendations are what I consider to be the current best approach. But that is my perspective, and indeed your experience, situation, and context may differ. With time these recommendations may also become dated, so as with most things in life, take the time to evaluate the information and determine if it makes sense for you and your objectives.

In developing this section, my thesis is that you cannot deploy software and call it a day. Instead, you are responsible for designing, developing, and deploying a world-class medical device cybersecurity program that would meet or exceed the FDA Medical Device Cybersecurity Regional Incident Preparedness & Response recommendations playbook first published in 2018 by the FDA and MITRE.

If that is your objective, then the items presented here will help you to achieve that goal. Even if that is not your objective, you will find that you will develop a much more mature and robust medical device cybersecurity program by considering each item in the following sections. To that end, we will consider what it takes to comply with best practices and regulations, detect threats and attacks and respond to incidents.

Ultimately addressing each of these areas will assure you can meet or exceed the FDA recommendations. Conversely, if you fail to balance and manage these areas, you could have a medical device cybersecurity program that is less mature and effective.

Comply – Our goal here is to identify those practices that allow us to comply with industry best practices (specifically medical device cybersecurity) and regulations (HIPAA).

Detect – We want to ensure that we can identify threats, vulnerabilities, and attacks but also want to be sure that we can take action regardless of the time of day or day of the week.

Respond – We want to assure that we can evaluate attacks and respond to them while doing all we can to ensure patient safety as best as possible.

Before we get into the specifics of what we should consider for the comply, detect, and respond buckets, we should take a step back. It is probably wise to have some "pocket questions" to help get colleagues on the same page. The purpose here is to create higher-level dialogue and demonstrate that a medical device cybersecurity program needs to be well thought out.

Consideration	Discussion
How does my medical device cybersecurity program integrate with my other IT security systems?	If you think back to the scenario we presented earlier, it is apparent that medical device cybersecurity is a team sport. It is not just clinical engineering or an IT Security effort. You need to determine how your strategy will work with your existing IT Security systems.
How do you create a common operating system?	Although an attacker may attack a medical device, it is more probable that the attack will start somewhere on your network or other devices. Having a common operating picture is crucial.
What unique expertise will you need?	It is essential to realize that even if you have a mature IT Security team, they may require additional training. Further, you will need to augment your clinicians' skills, rapid response team, and clinical engineering teams.
What specific policies and practices are required?	IT Security policies and practices focus on protecting assets (systems and data), and medical device cybersecurity is about protecting human life. It would be best if you made sure this difference is understood.
What happens if there is an incident?	Responding to a medical device cybersecurity incident is different from responding to a traditional IT Security incident. The use of specialized protocols and other techniques need to be evaluated and implemented.
Is this building a complete solution or just a single piece of the overall solution?	This question is critical to consider, especially considering all that has been reviewed in this manual.

Comply Considerations

These action items and considerations are designed to help you evolve your ability to comply with best practices and regulations.

Action Item	Consideration
Deploy Medical Device Specific Cybersecurity Policy and Practices	IT Security policies may apply to medical device cybersecurity. Still, often they do not address the specific requirements of this specialty area (training, qualifications, response levels, etc.)
Establish a Manufacturer Risk/Security Assessment Framework	You should develop a manufacturer assessment framework specifically for evaluating medical device risk and security.
Institute an "End of Life" Management Program	A good number of medical devices rely on end-of-life operating systems or software. A plan for transitioning these systems out of the environment should be developed to demonstrate ongoing risk management.
Determine a Medical Device Cybersecurity Team Model	You should identify who will participate in the primary and tertiary medical device cybersecurity teams.
Develop a Medical Device Threat Intel Program	You should identify the specific threat sources for medical device cybersecurity. Assure that you can explain why you choose these threat sources and how they are monitored.
Governance and Management	Determine your governance model and how you will specifically administer and manage your medical device cybersecurity program.

Detect Considerations

These considerations are designed to help you consider how you will detect and analyze threats, vulnerabilities, andpotential attacks.

Action Item	Consideration
Deploy Deep Packet Inspection Network Monitoring	Deep packet inspection is essential to monitoring network-based attacks and critical for medical device monitoring and fingerprinting.
Employ Deception Technologies	You will need to determine how you can protect devices from unknown attacks or activity on segregated networks. Integrated deception technologies are an essential consideration.
Utilize Host Intrusion Detection for Monitoring Stations	You should consider host-level monitoring for a medical device supporting infrastructure such as patient monitoring stations.
Assure Asset Fingerprinting and Management Systems are Deployed	Automated fingerprinting and classification of devices are essential for threat analysis and incident response.
Create a Vulnerability Assessment Program	A program to perform vulnerability assessments is critical. Do not just rely on "network-based assessments" but assure you have a program that performs targeted vulnerability assessments of representative populations.
Establish COP and 24x7 Monitoring	Assure that your medical device program integrates with the broader enterprise cybersecurity program. This process should yield a single common operating picture (COP) and 24x7 monitoring of the environment.

Respond Considerations

These considerations are focused on those items required to effectively respond to a medicaldevice cybersecurity incident.

Action Item	Considerations
Develop Medical Device Cybersecurity Incident Response (IR) Team	Develop or utilize a team specifically trained to respond tomedical device attacks – 24x7. This should ensure they can provide patient care and make decisions that consider patient safety.
Establish Medical Device Cybersecurity IR Protocols	Develop and deploy Rapid Response Protocols to address medical device cybersecurity IR
Train Medical Device Cybersecurity IR Team in Rapid Response	Train your team in Rapid Response
Test the Medical Device Cybersecurity IR Program Annually	Perform tabletop simulations to develop muscle memory and identify tipping points. Ensure all lessons learned are addressed. The tabletop should stress every area of your program, from policies to attack detection to fingerprinting to rapid response and patient safety.
Integrate Medical Device Cybersecurity IR with IT Security IR	Integrate your rapid response capability with your IT Security and other IR components, including disaster recovery and OEM.

Project Skeleton

A detailed project plan is well beyond the scope of this manual. Still, I did want to provide at least a starter set of tasks to consider as you move from envisioning your medical device cybersecurity program to planning and deploying. One of the most important lessons we have learned from working with our clients is to spend a considerable amount of time working through policies and procedures and establishing a cross- functional team that can support your efforts is crucial. Medical device cybersecurity is not an island, and having a cross-functional team (nurses, doctors, IT, clinical engineering, vendor representation, executive sponsorship,HR, legal, compliance, etc.) involved from the start will help to ease policy and procedure adoption, which ultimately should be the foundation of your program.

Although this skeleton plan is divided into three sections, you could refactor this to suit your needs. One key to success is thinking about medical device cybersecurity at your organization as a product, and this plan is for the development of your "1.0" release. Once you have the initial program deployed, you can then determine what is working well or needs to be optimized and begin working on your "2.0" release and beyond. Just remember that a medical device cybersecurity program is an ongoing and never-ending evolution.

Policy & Governance

This section focuses on developing your policy and procedural foundation. Establishing your cross-functional team, key objectives, and cadence are critical to success.

Project Task
Policy Draft Development
Policy Draft Review
Policy BETA Testing
Vendor Assessment Framework Draft
Vendor Assessment Framework Review
Vendor Assessment Framework BETA
Establish Governance Framework
Finalize Medical Device Security Policy 1.0
Finalize Medical Device Vendor Assessment Framework 1.0
Conduct First Medical Device Cybersecurity Governance Meeting
Patient Disclosures
Executive and User Education
Identify Current Medical Device Asset inventory

Security Architecture

Security architecture can mean different things in different settings. For this plan's purposes, we define security architecture as the standards and *practices required to safeguard patients connected to medical devices*. In short, this section should enable your policies and procedures to come to life and actually be employed day-to-day.

Project Task
Establish Medical Device Network Security Standards
Establish Medical Device Network Segregation Architecture
Develop Medical Device Evolve and Replace Strategy
Present Medical Device Network Plan and Architecture
Establish Medical Device Honeypot Program
Establish Medical Device Vulnerability Assessment Program
Perform Baseline Medical Device Vulnerability Assessment

Security Operations

This section focuses on how you will operate your medical device cybersecurity program 24x7. This includes the ability to respond to alerts, monitoring and integrate threat intelligence, indicators of compromise, manufacturer disclosures, and more. Further, you should be able to educate your end-users in anomaly detection and reporting and develop and train your rapid response program for medical device cybersecurity incident response.

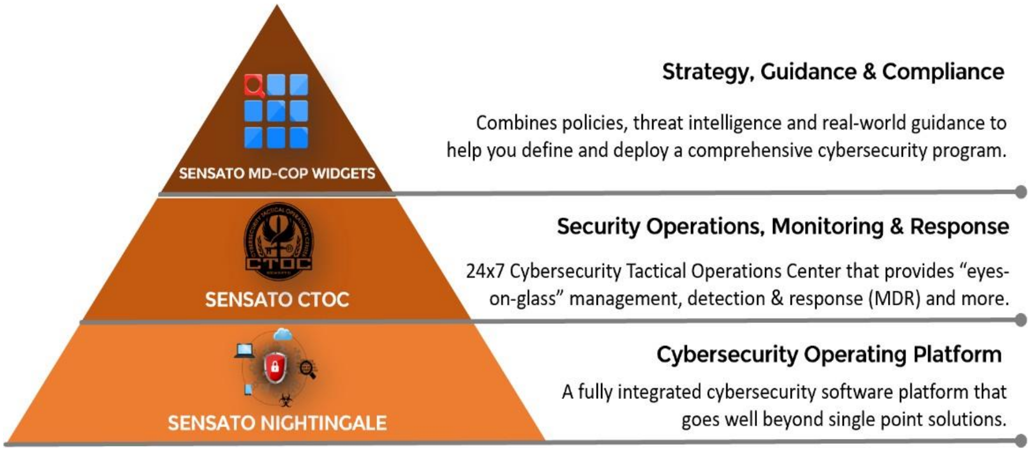
Project Task
Establish Medical Device Monitoring Program
Establish Threat Intelligence Program
Develop & Deploy a Medical Device Cybersecurity Rapid Response Team
Develop & Deploy Medical Device Cybersecurity Awareness Training Program

Sensato MD-COP

This manual has been focused on helping you design, develop, and deploy a holistic and effective medical device cybersecurity program. Hopefully, you have found the information presented to be meaningful, thought-provoking, and valuable. Suppose you decide that walking the path to achieving a holistic medical device cybersecurity program is not something you want to do alone. In that case, we do hope you will evaluate our Sensato MD-COP solution.

Sensato MD-COP goes well beyond the typical medical device cybersecurity program. In fact, Sensato MD-COP is the only medical device cybersecurity program to meet or exceed all the recommendations inthe FDA Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook.

That could be because many of the medical device cybersecurity best practices were pioneered by Sensato back in 2015. Sensato was the founding organization of the Medical Device Cybersecurity Task Force (MDCTF), which brought together eighty-three healthcare organizations, medical device manufacturers, MITRE, andindustry experts to develop practical approaches to holistic medical device cybersecurity programs. Today, **Sensato MD-COP is the only medical device cybersecurity program of its kind,** and is based on thought leadership developed by the members of the MDCTF.


SENSATO MD-COP WIDGETS
Strategy, Guidance & Compliance
Combines policies, threat intelligence and real-world guidance to help you define and deploy a comprehensive cybersecurity program.
SENSATO CTOC
Security Operations, Monitoring & Response
24x7 Cybersecurity Tactical Operations Center that provides "eyes-on-glass" management, detection & response (MDR) and more.
SENSATO NIGHTINGALE
Cybersecurity Operating Platform
A fully integrated cybersecurity software platform that goes well beyond single point solutions.

Sensato MD-COP brings together an amazing cybersecurity software platform, 24x7 medical device cybersecurity operations monitoring and response, policy and procedural templates, tabletop simulations, end-user training for awareness, and medical device incident response in a single unified solution.

Further, Sensato is one of the only cybersecurity firms that specialize in healthcare cybersecurity and is recognized as an Information Sharing & Analysis Organization (ISAO). We also respond to, develop, and support medical device cybersecurity tactics and strategies under our Memorandum of Understanding (MOU) with the U.S. Food and Drug Administration (FDA).

A Continuing Journey

The purpose of this field manual is to help you gain a foundational understanding of the components, practices, and perspectives required to design and develop a holistic medical device cybersecurity program. Even though the information presented here has been successfully used to deploy mature medical device cybersecurity programs at several hospitals, it is not the end of the journey. As threats continue to evolve and attackers become bolder and more daring, our ability to evolve will be challenged.

A well-designed foundation is critical to supporting the weight of the challenges that will arise and test this cybersecurity specialty. With time I foresee the need for cybersecurity clinicians, automated response to medical device security, FDA cleared security appliances, and more. An essential item that was not covered in this field manual is recovery and prolonged operations. Companies like Sensato and others are working hard to anticipate and address these challenges. Yet, the foundation you put in place today will be the difference between your ability to evolve in the future or find yourself going back to the drawing board.

If Sensato can be of assistance to you, please reach out. We are incredibly passionate about our mission and responsibility to the healthcare sector. Regardless, if you simply want to kick around an idea, talk about the future, or investigate deploying our MD-COP or other solutions, we would love to speak with and get to know you…our colleagues in the fight against those who would try to do patients' harm.

Reach Out to Sensato at:

✉ info@sensato.co

☎ 844.736.7286

🌐 www.sensato.co