Clearwater

Whitepaper

How an Integrated Risk Management Solution Can Help You Remain Compliant and Keep Medical Devices Safe

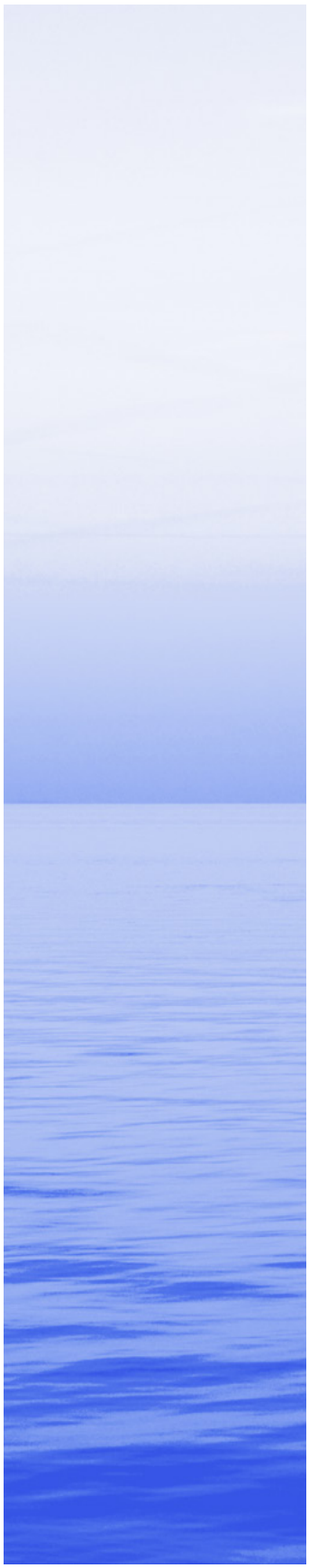
Table of Contents

Introduction

As the world becomes more interconnected through the use of network communications technology, we're likely to see—and benefit from—continued rapid innovation in medical devices and their capabilities across the healthcare industry.

Whether it's a wearable medical device that tracks heart rate and blood oxygen levels or more sophisticated devices like pacemakers and beyond, more and more companies are developing devices that rely on telecommunications and wireless connectivity to improve patient treatment, planning, and outcomes.

But these new capabilities also increase cyber risk and expand the threat landscape for medical devices. Devices that were once closely monitored and maintained only within hospital settings, now traverse a variety of networks and connectivity sources, leaving patients susceptible to risks, which, in the worst case, can result in death.



The current landscape

In the first half of 2020, the FDA cleared or approved more than 20 new medical devices, which reached nearly 40 by the end of August, following closely on the heels of the nearly 50 new medical devices and related technologies approved the previous year. These device types range from laboratory testing equipment to heart valves, nerve stimulators, and even connected devices implanted in the brain.

Industry experts anticipate continued growth for the Internet of Medical Things (IoMT), with the total global IoMT market estimated to reach nearly $160 billion by 2022, a significant jump from just three years ago when, in 2017, the market estimate was just north of $41 billion. The Asia-Pacific market will likely lead these gains, followed closely by North America and Europe respectively.

One of the driving factors for growth this year has been the coronavirus pandemic, which forced providers to find innovative ways to adopt and expand telehealth options. Connected devices, such as wearables with wireless monitoring, allow providers to continue continuity of services, without seeing patients face-to-face.

Here are some of the many benefits created by industry and consumer adoption of IoMT and Internet of Healthcare Things (IoHT):

- Ability to remotely assess and treat patients
- Ability to remotely and continuously monitor and evaluate patients, especially those with chronic diseases who may be home or facility-bound
- Improved patient outcomes
- Cost savings for providers, insurers, and patients
- Better patient experiences and improved satisfaction
- Improved diagnostics
- Improved treatment options
- Better and more streamlined case management, especially for those whose conditions warrant treatment across multiple disciplines for care continuity

Increased vulnerabilities

While these benefits fuel IoMT market expansion, expanding connectivity and increased usage adds a new layer of challenges and vulnerabilities for the healthcare industry, device manufacturers, and related and connected services.

Unfortunately, healthcare in the U.S. continues to lag behind most other industries when it comes to the areas of information security and cybersecurity. Considering the increasing number of devices and data breaches in the U.S. healthcare industry, it is no longer a matter of “if” a healthcare organization will come under a cyberattack, but “when”.

According to a 2019 HIMSS Cybersecurity Survey, more than 15% of significant security issues originated with either a medical device problem within the hospital or through a vendor’s medical device. Potentially even more alarming, it was reported that almost 70% of device manufacturers and 56% of healthcare organizations expect a device security breach during the next year.

That’s reflective of what’s being seen across the industry, with one report revealing that more than 80% of healthcare devices are at risk because of the coronavirus pandemic.

There are an estimated 10-15 million medical devices in use in hospitals throughout the U.S., a number expected to surpass 50 billion in 10 years. The situation is further complicated by the age of these devices. The average lifespan of a medical device in a typical hospital setting is 20 or more years. When you add to it that the average hospital room has upward of 15 connected medical devices, it’s not hard to see why the industry remains in the crosshairs of opportunistic hackers.

Adding yet another layer of complexity to risk is that almost all—98%—of IoMT devices are unencrypted, according to Palo Alto Networks Unit 42 2020 Threat report. As a result, more than half of healthcare IoT devices are vulnerable to attack straight out of the box, so to speak. Many of the attacks on unsecured and unencrypted devices originate with the exploit of a well-known vulnerability, even something as simple as the use of a default password that can be easily obtained from reading an installation guide or user manual.

And, across the healthcare industry, a convergence of traditional IT devices with IoMT devices, means there's an expanding attack surface where attacks can easily move undetected across networks and devices.

Cybersecurity Ventures went as far as to say that medical device exploits may be the single most dangerous cyber threat we will face in the next 10 years.

2020 risks at a glance

We mentioned earlier that it's no longer "if" medical devices may be hacked, but "when." Here's a quick look at some notable issues discovered this year:

- The Cleveland Clinic discovered vulnerabilities in Philips SureSigns VS4, a vital signs monitor that could leave the device susceptible to remote exploits, including improper input validation, improper access control, and improper authentication.
- NetWalker and DoppelPayer ransomware threat actors posted data from two healthcare providers and a device manufacturer to a dark web blog, including credit card authorization forms with contact information, payments, signatures, copies of IDs, and other sensitive medical data.
- Vulnerabilities discovered in Philips Dream Mapper software, used by sleep apnea patients, could facilitate an exploit allowing unauthorized access to log files.
- Vulnerabilities discovered in six medical device systems manufactured by Biotronik, Baxter, and BD Alaris could allow an attacker access to patient information and the ability to alter system configurations.

Where IoMT is vulnerable

- Device software
- Firmware
- Removeable media

- Device hardware
- Network access/firewall
- Operating system
- Ports/interface
- Remote support/maintenance
- Physical access
- Database and/or storage
- Clinical applications

Data for exfiltration

Vulnerabilities in IoMT devices expose a growing list of data types for patients and providers. In addition to personally identifiable information (PII) and protected health information (PHI), here are some other examples of sensitive data attackers could access through a successful medical device or medical systems exploit:

- Drug types and dosages
- Control information for diagnostic images
- Lab results
- Vital signs of all types
- Output from EKG and EEG and similar systems
- Data from implanted, connected medical devices

Security challenges

In addition to the volume and diverse asset types for medical devices across healthcare, there are a number of other issues that make medical device security difficult to manage, leaving these devices open to possible attacks.

Let's take a look at some of the most widespread issues for IoMT devices:

- **Lack of inventory**
  - Not visible in IT and security management systems
  - Lack of awareness of device cyber risk status

- **No patching**
  - Devices use old and often proprietary operating systems
  - Security patches are not pushed fast enough due to long validation processes and supplier dependency
  - Hesitation to patch for fear of shutting down a critical system
  - Fear patching could have negative impacts on patient safety
- **No risk analysis**
  - Threats are not evaluated
  - Lack of knowledge about which controls can reduce risk to acceptable levels
- **Complex management**
  - Not categorized in logical groups to facilitate comprehensive risk management or adequate security controls implementation
- **No risk management**
  - Device risk treatment not integrated into the organization's overall IT risk management
  - Creates an incomplete view of organizational risks
- **Insufficient controls**
  - Devices lack proper EDR, anti-virus, firewall, etc.
  - Network-based protections don't have required semantics or granularity
  - Unsupported operating systems don't have available updates
  - Cost considerations hamper the implementation of upgrades and security enhancements are delayed or thwarted during an analysis of risk vs. reward
- **Third-party liabilities**
  - Risks expand to third-party suppliers and vendors, for example, physical access database storage, clinical applications, and clinical application integrations
- **Insider threats**
  - Employees or contractors could be lured with financial payoffs for malicious activities
  - Risks created by human error or failure to follow policies
  - Lateral exploit movement that begins in IT (for example, a connected laptop) and then moves into IoMT devices or vice versa

Risk impact

It has been reported the healthcare industry has the heftiest average costs of a data breach—more that $7 million. However, as we mentioned before, and it's always worth emphasizing, the worst case scenario for a medical device exploit is not just the fines, penalties, and possible criminal or civil implications, it's potential patient death.

A single successful medical device breach could easily disrupt key functions for a device or facility. With lateral movement across your network and devices, it could shut down healthcare operations for a connected entity altogether. This can compromise data integrity, putting patients at risk.

And, as we have seen with data breaches across all industries, it can take almost 300 days to discover and contain a single breach. That means bad actors have plenty of time to enter your network through a compromised device and then move through your systems enabling further exploits while compromising data and patient safety.

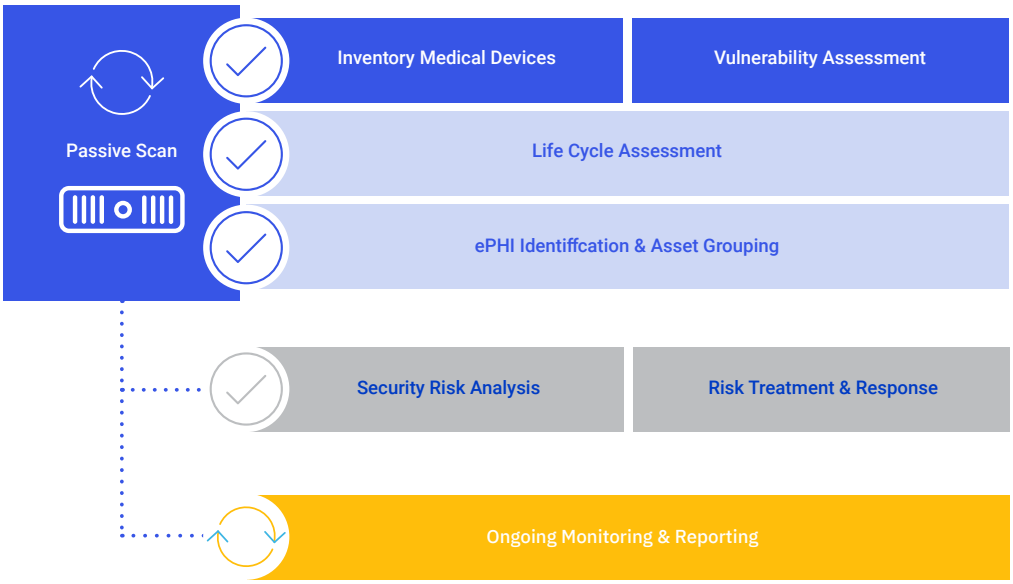
> NetWalker and DoppelPayer ransomware threat actors posted data from two healthcare providers and a device manufacturer to a dark web blog, including credit card authorization forms with contact information, payments, signatures, copies of IDs, and other sensitive medical data.

Building an automated defense for medical device lifecycle management

Let's explore what an automated defense for your medical device lifecycle might look like and how you can put this to work right away for your organization:

1. **Identify and assess medical device inventory.** Begin with your procurement process and identify where you purchased each device and indicate intended usage, but go further. It may be helpful to unite with a partner who specializes in medical device inventory. Not only can these specialists help you identify and inventory all of your devices, but they can also help you cull relevant device data to facilitate vulnerability assessment and vulnerability management for each device. Here are a few areas for review:
   - Which devices do you have?
   - What does each device do?
   - Where is each device located?
   - Who is responsible for device management?

2. **Adopt a risk analysis and risk management platform** to help you perform a security risk analysis, manage risk treatment and response, and collect data to inform ongoing device monitoring and maintenance throughout the lifecycle. Consider a solution that is both scalable and flexible to meet you where you are and change or grow with you over time. Seek out a solution that aligns with your organizational objectives and strategies. Don't just ask what the solution does. Dive into how the solution solves your specific challenges and facilitates success and security.



Components of an automated defense

Enterprise Cyber Risk Management software and software for medical device inventory can help you facilitate risk analysis and implement and document risk remediation plans for HIPAA compliance and security. Here are some key components your solution should employ to build your automated defense strategies:

1. **Inventory:** Comprehensive system inventory with device data at a granular level, including passive monitoring that interrogates the system without compromising system resources.
2. **Device profile information:** Medical devices don't have a lot of resources, such as power or storage. That means you can't implement (or it's difficult to implement) basic security measures such as encryption or anti-malware; however, deep packet inspection through the network can gather key information about network protocols and the device, including all its characteristics, as well as any device storage with characteristics of that storage. It's also important to be able to track data flow, for example:
   - What PHI goes into the system?
   - Is PHI stored on the device in any way?
   - Where is it stored?
   - Is PHI passing through the device to another device or system?
   - Where does that PHI go from there?

3. **Ability to address vulnerabilities and threats:** Employ a solution that's capable of continuous monitoring of all assets for threats and vulnerabilities, including event correlations, log analysis, and alerts for IoMT security.
4. **Data prioritization:** The ability to break through vulnerability overload and understand what you need to do with the data you discover, including the ability to easily prioritize risks for mitigation or remediation and facilitate actions to improve your overall security posture.
5. **Compliance support:** Ensure devices meet all regulatory and compliance standards, including documentation needed to support audits and reviews.

Medical device compliance

Both HIPAA and the FDA include medical device risk responsibilities and regulatory requirements.

For HIPAA, your security risk analysis must incorporate potential risks and vulnerabilities to the confidentiality, availability, and integrity of all ePHI your organization creates, receives, maintains, or transmits. (45 C.F.R. § 164.306(a).)

The FDA, as referenced in the HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework, recognizes that healthcare delivery organizations (HDOs) are responsible for implementing [medical] devices on their networks and may need to patch or change devices and/or supporting infrastructure to reduce security risks. Recognizing that changes require risk analysis, the FDA recommends working closely with medical device manufacturers to communicate changes that are necessary. So, how do you adhere to these requirements for medical device security and risk management? Here are some recommendations:

1. Develop a medical device management lifecycle plan, policy, and procedure
2. Implement a mechanism(s) to scan and identify a comprehensive medical device inventory
3. Perform a technical assessment of all medical devices required by 45 CFR §164.308(a)(8)
4. Perform a risk analysis and risk management activities on all groups of medical devices required by 45 CFR §164.308(a)(1)(ii)(A) & (B)
5. Perform ongoing auditing and monitoring on all medical devices with the highest levels of criticality

Guidance for risk analysis

If you need help performing a risk analysis, you may want to refer to guidance established by the Office for Civil Rights (OCR). OCR outlines nine process elements (regardless of risk analysis methodology). They include:

1. Analysis scope
2. Data collection
3. Identify and document potential threats and vulnerabilities
4. Assess current security measures
5. Determine likelihood of threat occurrence
6. Determine potential impact of threat occurrence
7. Determine risk level
8. Finalize documentation
9. Periodic risk assessment review and updates

Here at Clearwater, we suggest one more step: 10. Meet emerging OCR standards of care

It's important to point out here that for effective risk analysis, you should review each device or each device category at a granular level. You need to understand the device characteristics and related risks. And when it comes to protecting PHI, that includes all PHI devices, including traditional IT, your network, and infrastructure.

Also, don't forget to assess all of your third-party service providers and other IoT devices or integrated equipment within your organization that accesses, transmits, or stores PHI.

While compliance is a great reason to implement processes and procedures to protect all your medical devices, remember, there's a bigger picture here—protecting patient lives.

Conducting a risk analysis for medical devices

Risk analysis and risk management are vast processes, and if you're managing them with static documents like spreadsheets or paper reminders, you may put your organization at risk. You may find it more beneficial and efficient to adopt

a risk management platform to get true insight into what's going on within your organization. A risk management platform can give you comprehensive and clear insight into your organizational controls and safeguards, the effectiveness of those controls and safeguards, the ability to rate risks, and report on that risk grading, as well as continuously planning and evaluating your path forward.

And it's not just about completing an analysis. You also need support to conduct remediation, track that remediation, and understand your success points and weaknesses.

Here are a few recommendations to help you manage risks in a complex and evolving threat landscape for medical devices:

Risk Analysis Approach

- **Initiate**
  - Kickoff and introduce project
- **Plan**
  - Confirm initial scope, identify subject matter experts, establish and review plan for conducting risk analysis
- **Assess**
  - Collect information, identify potential threats and vulnerabilities, assess current security measures (controls)
- **Analyze**
  - Determine likelihood, impact, and level of risk
- **Deliver**
  - Document analysis and populate and/or update your risk analysis solution

Risk management

Improving your security process doesn't end with a risk analysis. Remember, your starting point was asset inventory with continuous monitoring and vulnerability analysis. But once you find a risk, what do you do? How will you fix it? This is where risk management comes in.

Risk management helps you compile your risk information in a way that you understand where your risks are and then enables you to build a roadmap to plan how you will address and remediate those risks and track your progress—not just to pass a compliance audit but to benchmark your progress internally so you can mature your processes and keep PHI and patients safe.

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact