EMERGING MEDICAL DEVICE CYBERSECURITY LEGISLATION

Guidance to help manufacturers develop secure, compliant medical devices

Introduction

It's a familiar scenario that has repeated itself many times. A particular industry produces a product or service that's in use by millions of people and, over time, it becomes apparent that use of the product involves risks — which may include physical hazards or security threats.

The very best manufacturers always respond comprehensively to fully mitigate the risks. Most manufacturers make at least some effort. Yet the known risks are never fully addressed because of factors such as economic imperatives or a lack of awareness.

In the next phase of this paradigm, government authorities publish advice for manufacturers, or develop regulations, depending upon the severity of the risks. Manufacturers must then adopt the advice or retrofit their products for compliance to ensure that their devices pass approval and to prevent potential legal action.

In this process, it has become clear that "best practice" guidance does not have enough teeth to get an entire industry to consistently mitigate against risk. Therefore, today governments are making a more proactive move from best practice guidance to enforcement by turning that guidance into law.

When that switch happens rapidly, as we're seeing in cybersecurity regulation for medical devices, it leaves manufacturers scrambling in the product design process. This can lead to failed product approval, product recalls and enormous financial consequences in the form of mitigation efforts, legal costs and lost revenue.

It's a challenge that medical device manufacturers need to take seriously, and with urgency. In this guide, Digi outlines the latest legislation and explains how medical device manufacturers can navigate the changing regulations to avoid a big hit to the bottom line.

Changing Risks, Changing Law

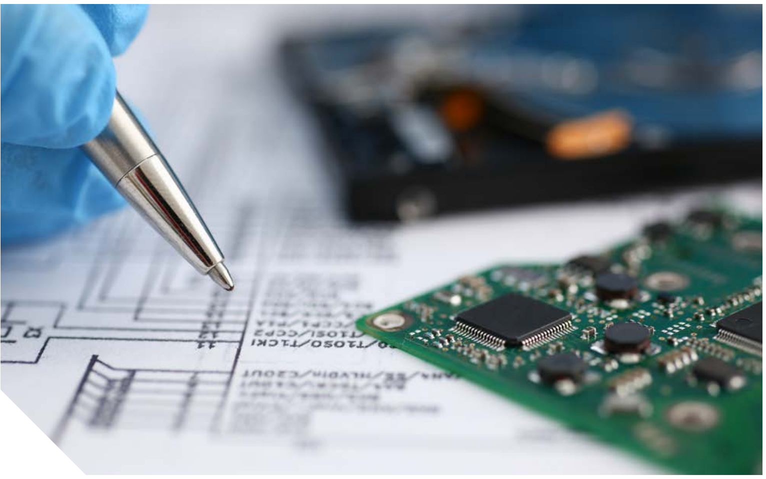
Not that long ago, medical devices that were connected to a provider's network were linked to an internal network that never connected to the outside world. Growing reliance on the Internet for communications changed all of that — and it's only accelerating with the IoT revolution.

Nowadays medical devices are routinely exposed simply because the internal network the device is connected to eventually joins up with the wider Internet. Even more concerning, many devices rely directly on the public Internet for communication, using Bluetooth or Wi-Fi to send data back to healthcare providers.

The result is that external actors located anywhere in the world can use automated attack tools to continuously probe a healthcare provider's network, including the medical devices attached to it.

Capterra's 2022 Medical IoT Survey underlines the growing size of the risk. The survey found that the more connected devices a healthcare establishment relies on, the higher its risk of a cybersecurity attack. Respondents in that survey also stated that 48% of attacks had an impact on patient care (and 67% had an impact on patient data).

Equally alarming, research by Unit 42 at Palo Alto Networks found that 75% of more than 200,000 infusion pumps examined showed that the infusion pump had a heightened risk of being compromised.



Understanding the Risks

The medical Internet of Things (IoT) is contributing to effective and patient-centric healthcare, but there are also inherent risks to the security of healthcare institutions and even the well-being of patients. These risks come from a wide range of sources. Internet-connected or "smart" medical devices are vulnerable to a variety of attacks that compromise their functionality, accuracy, and patient safety. The following are some noted examples.

- **Data breaches:** Connected medical devices store and transmit sensitive personal and medical information and are a prime target for cybercriminals looking to steal patient information. A data breach can result in the exposure of patient data such as social security numbers, medical histories, and insurance information.
- **Tampering and hijacking:** Attackers can manipulate or tamper with the functionality of connected medical devices, potentially altering performance and leading to incorrect diagnoses or treatment. That includes a denial of service (DoS) attack that can disrupt a device by compromising its performance, but also instances where hacked devices are used to launch a distributed denial-of-service (DDoS) attack, in which the victim becomes a vicarious perpetrator — flooding other targets with incoming traffic.
- **Malware infections:** Malware can infect connected medical devices and spread to other devices within the healthcare network, leading to widespread disruption and potentially putting patient safety at risk.

The breadth of the risk and the potential gravity of a successful attack means that healthcare organizations and device manufacturers must take steps to secure connected medical devices and protect patient information from cyberthreats. That includes strong security measures, such as encryption and secure authentication, but also regularly updating software and firmware to fix emerging vulnerabilities.

Legislation Is Responding

The cybersecurity risk to medical devices is not coming as a surprise. Major warnings and recall events include FDA warnings about infusion pumps, pacemakers, and insulin pumps — some of which required recalls.

Warnings and recalls can lead to widespread anxiety and disruption in the healthcare setting — even if no patients were harmed. Manufacturers have been aware of the cybersecurity risks for some time, and so have the buyers of medical devices.

Governments and regulatory bodies know about the risks too. Good practice and advisory documents covering medical device security have been around for about a decade.

For example, back in 2014, the U.S. Food and Drug Administration (FDA) produced an advisory document titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices".

Nonetheless, good practice and advice apparently lacked sufficient impact. The recall incidents pointed to the need for more concrete action.

Committing connected device security requirements into law — the same way law enforcement put speed limits into law rather than rely on signs alone — was clearly the next step.

Case in Point: FDA Powers

The story of how growing concern about medical device cybersecurity is moving from advisory regulation to law is perfectly illustrated by an action taken by the US government.

Right at the end of 2022, a 4,100-page omnibus bill that confirms ongoing funding for the US government was signed into law. And here's the pertinent part: the 2022 omnibus spending bill included a section that amends FDA law to now include key provisions covering medical device cybersecurity. However, there were several initiatives leading up to that change.

The FDA's Existing Power

In the US, the FDA already played a crucial role in regulating connected medical devices, covering both pre-market approval and post-market surveillance. For more information, see the Cybersecurity Safety Communications and Other Alerts section on the FDA website which lists recommendations for safety communications and alerts that healthcare facilities can adopt to reduce the risk of unauthorized access.

For pre-market approval, the FDA evaluates the safety, efficacy, and security aspects of connected medical devices through a rigorous review process. Manufacturers must submit detailed information about their device, including data from testing and clinical trials, and the FDA may require additional testing or information before approving a device for the market.

Once a connected medical device is on the market, the FDA continues to monitor it to ensure that it remains safe and effective. The FDA has several tools for post-market surveillance, including monitoring adverse events and issuing recalls if necessary.

FDA U.S. FOOD & DRUG ADMINISTRATION

Unsuccessful Efforts to Increase FDA Powers

The last large piece of formal cybersecurity guidance from the FDA was issued in 2014. Given the speed at which cybersecurity moves, there have been several efforts to update it — but these efforts either stalled or are still in the works. For example, a process is in place to update the 2014 guidance.

In April 2022 the FDA published a document called "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions — Draft Guidance for Industry and Food and Drug Administration Staff." However, at the publication of this white paper, the guide was still in a draft state.

Also, over the course of 2022, a number of bills were introduced in Congress that sought to empower the FDA to enforce rules on medical device cybersecurity. However, the bills did not manage to generate sufficient support, and a bipartisan bill called the Protecting Our Ability to Counter Hacking (PATCH) Act failed to gain traction.

To a degree, the FDA already had significant impact, as the agency could query a manufacturer as part of its Quality System Regulation (QSR) test that must be met in a 510(k) submission. And there are cases where the FDA rejected the cybersecurity content of a pre-market submission.

Guidance is, however, not the same as requirements that are written into law.

Key Medical Manufacturing Changes Buried in a Big Bill

Toward the end of 2022, Subchapter A of Chapter V of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 351 et seq) was amended by adding a clause for connected requirements (on page 3,537, line 18). The content written into law is relatively straightforward, and centered around a few key points, which can be summarized as follows:

- A medical device manufacturer must submit a plan to monitor for and identify cybersecurity vulnerabilities and exploits — including a plan to address these vulnerabilities and to commit to a coordinated vulnerability disclosure program — once the device is released to the market.
- The device manufacturer needs to design and maintain procedures that ensure devices are cyber secure when released to the market and also ensure that there is a path to patching devices once these products are in the market.
- There must be a commitment that non-critical patches are applied at a regular cycle, and there must be a route to address critical vulnerabilities outside the regular patching cycle.
- Manufacturers must publish an SBOM (software bill of materials) that covers all included commercial and open-source software components.

There is also an open-ended clause that says that a manufacturer must comply with any other requirements that the government may put in place in follow-up regulation. This latter point is extremely important in that it means that OEMs will have the responsibility to implement security changes that are not yet identified.

Signed into law on 29 December 2022, the new rules came into effect at the end of March 2023. The net result is that, with little warning, medical device manufacturers are now required by law to demonstrate to the FDA the cybersecurity capabilities of connected medical devices, and provide evidence of a plan to detect, address, and rectify any emerging cybersecurity issues — and to do so before approval is granted for the device.

> The FDA requires medical device manufacturers to publish an SBOM (software bill of materials) that covers all included software components. This requirement has been written into law and is now in force.

What About Global Legislation?

The FDA is a significant and important voice and, of course, where manufacturers sell into the US market, the FDA's guidelines should be considered throughout the product development process.

Nonetheless, there is much more regulation out there covering the global market for medical devices. Manufacturers operating in the rest of the world, as well as US-based manufacturers that want to sell globally, must adhere to at least some of these laws too.

European Union Law: RED or Not RED?

The EU connected devices law that's captured much attention recently is the EU's Radio Equipment Directive (RED). That said, this directive applies to medical devices only under specific circumstances. The EU regulations for medical devices (MDR) and in vitro diagnostic describe EU legislation with cybersecurity directives that focuses directly on medical devices.

However, most medical device manufacturers will also be covered by the NIS2 Directive, which **entered into force in January 2023**. Furthermore, the General Data Protection Regulation (EU) **2016**/679 (GDPR) and the EU Cybersecurity Act (Regulation (EU) **2019**/881) will also apply to some devices.

There are also uncertainties around the applicability on medical devices of the "Cyber Resilience Act" or CRA. The CRA is underway with a draft document ready, and while the medical devices industry is out of scope as it stands, signs are that this may change. Nonetheless, the following three groups of laws are particularly noteworthy.

Radio Equipment Directive

The EU's Radio Equipment Directive (RED) is not aimed specifically at medical devices. But RED rules do apply to medical devices if a medical device contains radio equipment components, such as Bluetooth or Wi-Fi modules, regardless of whether said device is finally interconnected or not.

This means that in some cases manufacturers need to design for conformity with both MDR/IVDR and RED. Medical devices that fall under RED include implants that can be controlled via an app, mobile patient monitors that send data using cellular, and devices that transmit data via Wi-Fi, for instance.

On the other hand, a medical device that only communicates through wired connections, like LAN, RS-232, or CAN bus, may be exempt from RED. Either way, RED article 3.3(d), (e) & (f) for cybersecurity is now in force. These points state that, from the **1st of August 2024**, for certain products, the manufacturer needs to ensure that the device:

- Does not harm the network or its functioning nor misuses network resources, thereby causing an unacceptable degradation of service
- Incorporates safeguards to ensure that the personal data and privacy of the user and the subscriber are protected
- Supports features ensuring protection from fraud

These are less detailed and exhaustive requirements compared to, for example, FDA guidance, but the EU RED requirements nonetheless do apply to medical devices that fall under its remit.

> EU's Radio Equipment Directive (RED) does apply to medical devices containing radio equipment components, such as Bluetooth or Wi-Fi modules.

MDR and IVDR

In the European Union, the primary rules for cybersecurity in medical devices are outlined in MDR Annex I Section 17.2 and IVDR Annex I Section 16.2. Similar to FDA rules, MDR includes points around post-market surveillance and incident reporting, as well as traceability and reporting around third-party software.

It is worth mentioning that according to the document "EU MDCG 2019-16 Rev.1 Guidance on Cybersecurity for Medical Devices" endorsed by the Medical Device Coordination Group (MDCG), it is clearly stated not to use end of life (EOL) third-party components and devices on the operating environment. Failure to comply with this requirement would result in the rejection of approval to introduce a new medical device to the European market.

The legislation requires that the product development process must take into account the entire product lifecycle as well as risk management and broader information security principles. MDR demands a verification and validation process too.

Under MDR and IVDR, testing is the primary means of security validation, using techniques including security feature testing, fuzz testing, vulnerability scanning, and penetration testing. Finally, MDR demands that medical devices must be as "autonomous as possible" in terms of IT security.

> European legislation is very explicit. Medical device manufacturers are required not to use end-of-life (EOL) components under any circumstances.

NIS2

The revised NIS Directive now includes a specification that classifies manufacturers of medical devices under the directive's list of "important entities." Furthermore, manufacturers of any medical devices that are critical for use in a public emergency fall under the "essential entities" remit of NIS2.

In turn, entities classified as "important" or "essential" — including medical device manufacturers — must supervise the implementation of cybersecurity risk management measures and may face consequences for non-compliance.

The NIS2 Directive also requires covered entities to report cybersecurity incidents in a staggered timeframe. The reporting process starts with an "early warning" within 24 hours of becoming aware of significant incidents, followed by an incident notification within 72 hours, and an interim report upon request.

> Under NIS2, medical device manufacturers must supervise the implementation of cybersecurity risk management measures.

Other Countries

When it comes to medical device cybersecurity, the FDA and the EU are two of the most influential regulatory groups in the world, but of course many other countries have their own regulatory rules for medical devices.

While we can't exhaustively discuss every regulatory ruling, we'll point to a few examples of medical device cybersecurity regulation in countries outside the US and EU — though the list of examples only grows once broader connected device legislation is considered.

Singapore

The Health Sciences Authority (HSA) of Singapore issues guidelines on cybersecurity for medical devices, covering the importance of cybersecurity risk management and the adoption of a proactive and ongoing approach to cybersecurity.

HSA guidelines require that medical device manufacturers assess the potential cyber risks associated with their devices, implement appropriate security measures, and provide regular security updates to address emerging threats.

Australia

In Australia, the Therapeutic Goods Administration (TGA) guidelines emphasize the importance of addressing risks throughout the device lifecycle. The organization focused on the importance of applying security update patches to mitigate the sheer number of attack strategies, as well as the application of appropriate security policies that include a thorough evaluation of the possible real risks for both medical devices and patients.

Brazil

Brazil's National Health Surveillance Agency (ANVISA) similarly issued regulations on cybersecurity for medical devices, requiring that manufacturers protect against unauthorized access, alteration, or destruction of data.

The regulations also require that manufacturers conduct risk assessments, provide regular security updates, and cooperate with other stakeholders, including healthcare providers and government agencies, to address cybersecurity threats.

IoT Cybersecurity Standards Behind Legislation

It's worth noting that some of the regulations and guidelines summarized in this section are based on existing IoT cybersecurity standards such as EN 303 645 and IEC 62443-4-2.

Therefore, it's advisable to take broader IoT security standards into account when evaluating the design of connected medical devices.

Particularly for products that will be shipped to Europe in 2024 and later, manufacturers should seek proof that their products meet these standards or obtain a third-party certification as needed.

As for the US, there is also the NIST Cybersecurity for IoT Program, NISTIR 8259A: Core Device Cybersecurity Capability Baseline (May 29, 2020) which should be considered by manufacturers of connected medical devices.

A Broad Set of Overlapping Laws: The Implications for Manufacturers

Faced with a tidal wave of legislation, what can medical device manufacturers do to manage their cybersecurity compliance obligations? Finding out which laws apply is a start, but that is also a challenge in its own right.

That said, a broad view of the principles behind the legislation can help, as these lead to design principles that device manufacturers can include in the design process. The most important step? Acting rapidly.

A Need to Rapidly Counter Risks

Whichever jurisdiction they're in, no manufacturer can wait until the development of the next generation of devices kicks off before they respond. The legislative clock is ticking. Medical device manufacturers must integrate the requirements of the regulation now because the risk of proceeding with a product that does not meet the latest cybersecurity standards is considerable:

- **Products may not pass approval:** While a product may have been designed for approval success as it stands, the rapid pace of change in the law can mean that a product fails at the approval stage — delaying product release.

- **Increased risk of cyberattacks:** Where manufacturers don't comply with medical device cybersecurity regulations, devices may be more vulnerable to cyberattacks, which could compromise the security and privacy of a patient's sensitive medical data, compromise the healthcare organization's network, its operations, and more.

- **Legal liability, fines, and penalties:** A manufacturer could face legal liability if a medical device causes harm to a patient due to cybersecurity breaches. That could involve a costly lawsuit that damages a manufacturer's reputation, or fines and penalties from bodies such as the FDA.

- **Loss of business, damage to reputation:** A single product recall and the associated media attention could be all it takes to substantially undermine future business. Once trust is lost in a manufacturer's devices, it can be difficult to recover.

- **Risk to insurance payouts:** Products that do not comply with cybersecurity advice or legislation may be uninsurable, and where the medical device did obtain insurance coverage there is a risk that an insurance payout would be refused if the insurer deems that a product was non-compliant.

The consequences of non-compliance with cybersecurity legislation are so significant that it may be advisable for manufacturers to consider retrofitting products that are near release — even if these products have passed the necessary approval steps.

Parsing the Rules

As a next step, medical device manufacturers need to understand which laws cover their devices. What is the new regulation about — and how does it fit in with their current modus operandi? How can a manufacturer get the design right from the start — without being told to go back to the drawing board at some stage during the approval process?

Jurisdiction is one obvious component. The other is whether a device falls under IoT and connected device regulation in addition to medical device regulation. Where a medical device is classified as a connected device, the manufacturer may need to take the view that cybersecurity legislation for connected devices also applies, in addition to medical device cybersecurity legislation.

Dates on which new legislation goes into effect also matter. New laws may have clear provisions on compliance for devices released after a specific date, but it is not always straightforward. Manufacturers must seek advice to understand whether a device falls under a new law.

Legislation can also apply to devices already in the market: legal bodies can add supplementary provisions to regulations to promote the renewal of existing devices and ensure necessary security enhancements.

Three Key Themes

Each of the cybersecurity rule sets has a long list of requirements stretching across pages and pages. That's presumably no problem if you're a specialist lawyer working in medical device approval.

But it makes it difficult for engineers, their supervisors, and the C-Suite to understand what it really comes down to. With such a long list of requirements, it helps to approach regulation from a broader perspective.

We suggest that medical device manufacturers can conceptually divide new cybersecurity legislation around three key themes or targets: Total product lifecycle, design transparency, and post-market responsiveness.

Medical device manufacturers can divide new cybersecurity legislation into three key targets: Total product lifecycle, design transparency, and post-market responsiveness.

1. **Total Product Lifecycle**

   One of the key changes in the latest cybersecurity laws is that manufacturers are now responsible for managing the cybersecurity of the product through its entire lifecycle. Simply releasing a product that is known to be secure at the time of release is no longer enough.

   Instead, from a cybersecurity perspective, manufacturers are now responsible for what happens to a medical device once it's in the field, in the home or in a clinical setting. That means that manufacturers need to design products for the cybersecurity future — including the ability to adapt products already deployed and in use to counter new cybersecurity threats.

2. **Transparency Throughout**

   The cybersecurity threat is now so large and diffuse, and the technology so integrated, that attempts to run cybersecurity in a "silo" are bound to fail. This is why new regulation is demanding that manufacturers are more transparent about the technology included in a product.

   Transparency is also needed upon the discovery of any vulnerabilities so that users and other partners can make a judgment about how a vulnerability affects their operations — and to close the risk that a manufacturer may stay quiet about a known vulnerability.

3. **Post-market Responsiveness**

   Finally, it is imperative that manufacturers can actively monitor and govern their products once they are out in the market. It includes relentless connectivity and management, as well as the ability to ensure that patches can be applied to a product.

Practical Steps for Compliance

Developing a device that complies with reams and reams of cybersecurity legislation might seem impossible but, in some ways, it is not that different from following any other product design specifications — as long as the manufacturer knows what the specifications are and uses the right tools.

Staying compliant therefore requires a grounding in medical device cybersecurity law and partnering with the right vendors to fill in the gaps. In this section we'll drill down to the practical requirements common to the various cybersecurity laws — and what device manufacturers need to do to meet these requirements.

Cybersecurity Built into the Design Process

Whether you call it Secure by Design, DevSecOps (development, security, and operations) or — as preferred by the FDA — a Secure Product Development Framework (SPDF), the goal remains the same. Product designers must think about cybersecurity as a foundational aspect of product design; and designing for security needs to be integral to the product development process.

That includes building a view of the security architecture of a medical device, including the interconnectedness of the device as well as the defenses and responses in place to prevent harm to multiple patients.

Risk Management Approach

Some advisory documents — including from the FDA — recommend that manufacturers conduct assessments to comprehensively identify and manage patient safety risks.

In managing these risks, device manufacturers must also at all costs avoid inadvertently introducing new risks. The outcome of the risk management process must be documented, and manufacturers need to maintain this documentation throughout the lifecycle of the device.

Threat Modeling

Threat modeling is a structured process with four objectives:

1. Identify security requirements
2. Pinpoint security threats and potential vulnerabilities
3. Quantify threat and vulnerability criticality
4. Prioritize remediation methods

As part of the risk management approach, some of the new regulation requires threat modeling. Here, manufacturers must follow a process (or work with a partner) that can assist in identifying security objectives, risks, and vulnerabilities across a medical device.

In fact, including a threat modeling report may be a requirement of the pre-market submission under some regulatory rules.

Threat modeling activities can be performed during design reviews and benefit from regular updates. One option is to use automated vulnerability assessment tools that can keep pace with a rapidly changing product.

Pro-active and Informed

Designing secure connected devices requires a proactive approach. Due to the complexities involved and the unique skills required, many organizations lack the internal resources and expertise to implement the tools and best practices for scalable IoT security.

Hence, the most advisable option is to partner with a trusted vendor who has sufficient experience and engineering staff specialized in the conscientious assessment of common vulnerabilities and exposures (CVE).

This is where Digi can provide the tools and the expertise to support seamless integration of best practices in the development, manufacturing and deployment of secure embedded devices. The remainder of this white paper provides guidance from Digi's embedded security experts and describes our total lifecycle approach to embedded device security.

Essential Cybersecurity Practice for Connected Device Design

We've discussed many different emerging regulations in this paper, along with the risks medical device OEMs need to assess and manage in the process of developing and maintaining connected products. Now let's talk about putting these into practice.

It's important to note that a new, broader approach to cybersecurity doesn't mean that more established and hardware-based cybersecurity principles are any less important. For example, device designers must consider the physical security of a device too — and avoid the temptation to use things like universal default passwords.

In practice, it means that device hardware must use secure boot including firmware validation, and any ports must be hardened. Network authentication and secure online connections are other key essential elements.

Update Encryption Post-market

Encryption across device operations — from hardware to network communication — is still a core tenet of medical device security and device manufacturers must make use of encryption wherever data is transmitted and stored. This includes both payload and headers, and applies to data in transit and at rest, to ensure that even if the data is intercepted, it cannot be read, used, erased, or altered.

However, threat actors are regularly breaking encryption technologies, requiring frequent updates to encryption algorithms. To ensure sensitive data is securely protected, and to meet compliance requirements, device manufacturers must build the capability to update encryption mechanisms into their field-deployed devices.

SBOM — Best Practice for Software Security

A “software bill of materials” (SBOM) has emerged as a key building block in software security and software supply chain risk management. An SBOM is a complete inventory comprising a list of ingredients that make up software components.

An SBOM helps identify devices affected by software vulnerabilities and facilitates risk-management processes. SBOMs are gaining popularity and are now included in compliance standards, as aforementioned, in the most recent regulation from the FDA, because of their traceability benefits.

For example, if a flaw in a widely-used open-source package is identified, the manufacturer (or at least the user) can rely on an SBOM to understand that a medical device is affected by the vulnerability and arrange for mitigation.

For medical device manufacturers, it is therefore now imperative to build and maintain an SBOM through the design process and keep it updated throughout the product lifecycle — as well as using automated mapping tools to ensure that an SBOM has been thoroughly analyzed. The OEM can also put this trust in the expertise of a vendor such as Digi at the forefront of cybersecurity.

Post-market Surveillance Plan

Manufacturers need to implement a post-market surveillance plan for medical devices to monitor the safety, security and performance of their products once in the market. That includes activities such as monitoring adverse events and complaints, conducting field corrective actions, and assessing the need for further clinical studies.

Post-market surveillance is at the core of the total lifecycle approach to cybersecurity. Using a robust and flexible cloud platform that connects to devices can help manufacturers accomplish this goal. Medical device manufacturers also need ongoing monitoring of cybersecurity vulnerabilities based on the SBOM to ensure that any software vulnerabilities are patched at an appropriate stage to mitigate risks with the minimum possible downtime.

Vulnerability Management Plan

A vulnerability management plan now commonly needs to be included in pre-market submissions. The plan should include elements such as identifying vulnerabilities, periodic security testing, and communicating with customers about updates and patches.

At the core lies the ability to patch a device once it is in the market — including the ability to apply an over-the-air (OTA) patch to rapidly respond to any new vulnerabilities.

Network Protection

It is particularly important, whenever a medical device could be classified as an IoT device, for the OEM to apply principles that ensure network protection in order to meet the demands in the EU’s Radio Equipment Directive and any other applicable regional requirements.

That includes features that avoid harming communication networks and disrupting their functionality by meeting technical standards and requirements. However, it also includes broader principles — for example, ensuring a device cannot be used as part of a denial-of-service attack.

Protecting Personal Information

Finally, as a core part of cybersecurity practices for medical devices, manufacturers must focus on protecting personal information — both to meet broader cybersecurity compliance regulations, but more specifically also to meet regulations such as the Health Insurance Portability and Accountability Act (HIPAA) or GDPR, both of which dictate how personal information should be protected.

In practice, that means implementing strong access controls through strong passwords and multi-factor authentication (MFA), using the encryption methods discussed. It also includes an important focus not just on device security, but on the entire platform — including any cloud infrastructure that supports device operations.

Partnering for Cybersecurity Success

The extent of medical device cybersecurity legislation is leading to a point where the efforts involved in meeting cybersecurity regulations have become a very cumbersome part of product development.

One way forward is adopting the right partners and toolsets — just as it is anywhere else in the product development process.

With the right tools, manufacturers can continue to develop products that meet the needs of patients while also meeting new and emerging cybersecurity regulatory requirements.

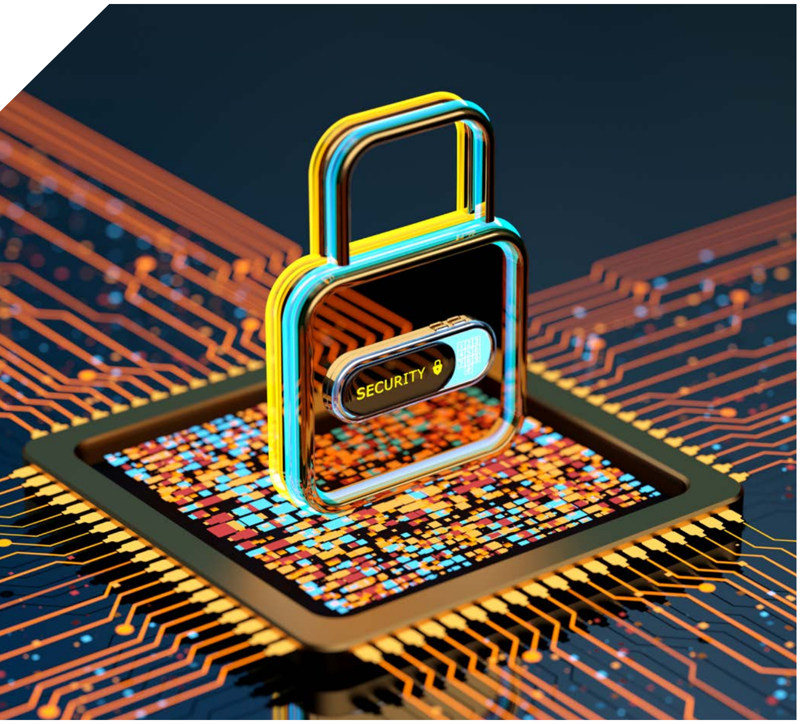
Cybersecurity Solutions for Medical OEMs

Taking the right measures during the design phase of a medical device can help ensure that device will remain secure throughout its lifecycle. That's a key step change from the current paradigm where many devices are released with cybersecurity flaws — and there is no ability to remediate risks after shipment.

While no one can predict novel cybersecurity threats, Digi solutions can help you prepare for them, and respond to emerging issues with agility. Digi embedded systems enable you to design devices with built-in cybersecurity responsiveness, integrate the ability to monitor device behavior in the field, and update devices against critical cybersecurity attacks long after these devices have been shipped.

Today, the cybersecurity threat is so vast that no single party can comprehensively monitor and manage all the cybersecurity concerns across a complex device. That's why transparency and responsiveness are critical.

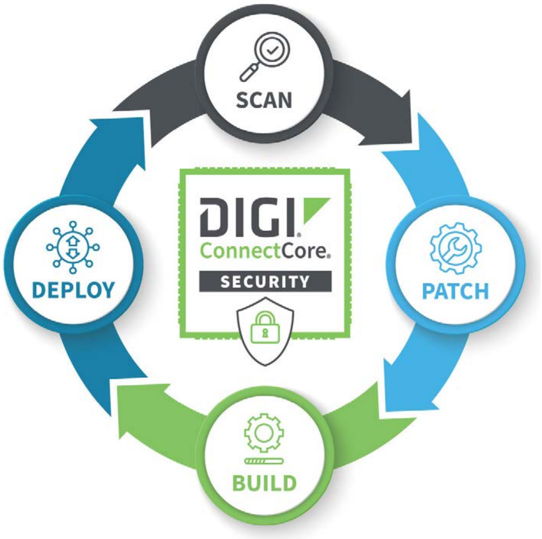
Digi helps medical devices OEMs to be fully transparent about what's included in a device through an SBOM, and act quickly when a vulnerability does emerge.



Digi Tools and Services for Secure Connected Medical Devices

Digi offers a full suite of edge-to-cloud connectivity products, services and tools, including system-on-modules (SOMs) and security and cloud services that aid medical device manufacturers in creating secure connected devices with remote capabilities and proactive management services.

Our services provide custom interfaces for the configuration, monitoring, and maintenance of connected devices and allow for automated processes that reduce costs and enable compliance.



Digi TrustFence

Digi TrustFence® is a security framework for mission critical IoT devices, including medical devices. It provides device security, device identity, and data privacy capabilities through features such as secure boot, protected hardware and ports, and network security. TrustFence uses the latest encryption protocols for data in motion.

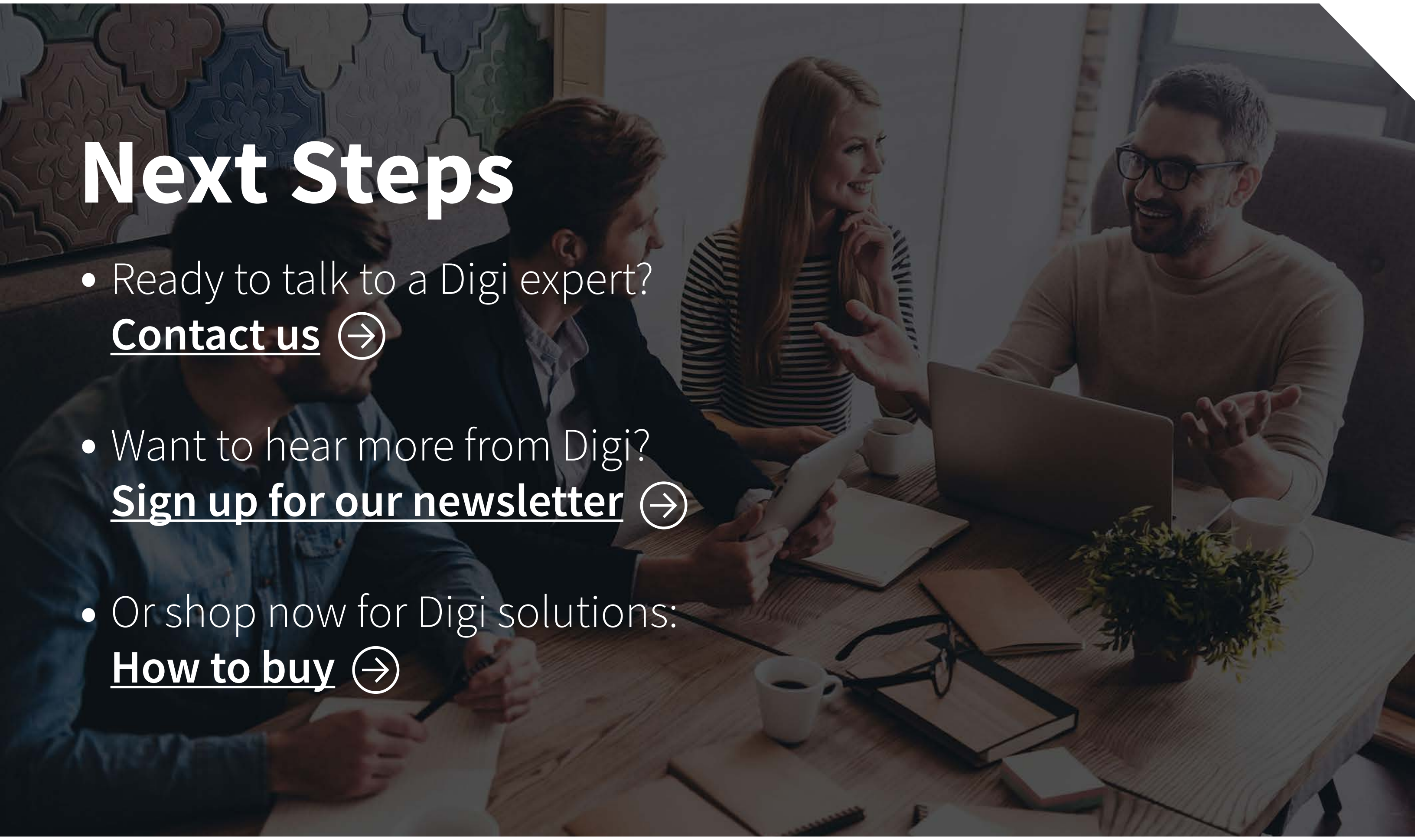
Digi ConnectCore Security Services

These services include a range of tools to monitor and analyze security risks and vulnerabilities throughout the product lifecycle.

Digi ConnectCore® Security Services include the analysis and monitoring of a custom SBOM and binary image running on Digi ConnectCore® SOMs for security vulnerabilities. To help remediate identified issues, the services provide a curated vulnerability report highlighting critical concerns, a security software layer including patches for common vulnerabilities, and consulting services.

Digi ConnectCore Cloud Services

Managing and monitoring devices once a device is in service in the clinical setting is critical. Digi ConnectCore® Cloud Services allow OEMs to create connected medical devices with remote dashboard and application capabilities. These services enable secure over-the-air software updates supporting process automation, remote deployment management, and cost reduction — and the opportunity to improve product quality, technical support and customer experience.



Next Steps

- Ready to talk to a Digi expert?
  Contact us →
- Want to hear more from Digi?
  Sign up for our newsletter →
- Or shop now for Digi solutions:
  How to buy →

Why Digi?

Digi is a complete IoT solutions provider, supporting every aspect of your project, from mission-critical communications equipment to design and deployment services to get your application designed, installed, tested, and functioning securely, reliably and at peak performance.

Digi builds its products for high reliability, high performance, security, scalability, and versatility so customers can expect extended service life, quickly adapt to evolving system requirements, and adopt future technologies as they emerge. Digi embedded modules, routers, gateways, and infrastructure management solutions support the latest connected applications across verticals, from the enterprise to transportation, energy, industrial and smart cities use cases.

Our solutions enable connectivity to standards-based and proprietary equipment, devices, and sensors, and ensure reliable communications over virtually every form of wireless or wired systems. Our integrated remote management platform helps accelerate deployment and provide optimal security using highly efficient network operations for mission-critical functions such as mass configuration and firmware updates, as well as system-wide monitoring with dashboards, alarms, and performance metrics.

Company Background

- Digi has been connecting the "Internet of Things" — devices, vehicles, equipment and assets – since 1985
- Digi is publicly traded on the NASDAQ stock exchange: DGII
- Headquartered in the Twin Cities of Minnesota, Digi employs over 800 people globally, and has connected over 100 million devices worldwide

As an IoT solutions provider, Digi puts proven technology to work for our customers so they can light up networks and launch new products. Machine connectivity that's relentlessly reliable, secure, scalable and managed — and always comes through when you need it most. That's Digi.

Learn more on our About Digi page.

Contact a Digi expert and get started today

PH: 877-912-3444
www.digi.com

Digi International Worldwide Headquarters
9350 Excelsior Blvd. Suite 700
Hopkins, MN 55343

/digi.international   @DigiDotCom   /digi-international

While every reasonable effort has been made to ensure that this information is accurate, complete, and up-to-date, all information is provided "AS IS" without warranty of any kind. We disclaim liability for any reliance on this information. All registered trademarks or trademarks are property of their respective owners.