RUNSAFE
SECURITY

Key Aspects of Medical Device Software Security

RunSafeSecurity.com

Table of Contents

Executive Summary

Modern healthcare settings are full of devices that use software to manage and improve patient care, from MRI machines to CT scanners to infusion pumps. However, while the integration of software into medical devices has expanded diagnostic and treatment possibilities, the advancements come with significant cybersecurity challenges.

Today, medical device manufacturers (MDMs) are responsible for both designing secure devices and for maintaining and updating security throughout the device lifecycle. By focusing on software security best practices, MDMs will be better able to protect patient data, device functionality, and, ultimately, patient safety from development to release to the market.

In this white paper, we'll explore critical aspects of medical device software security, covering risks to devices, regulatory frameworks, secure development practices, lifecycle considerations, and security protections that continually defend devices. By outlining best practices, manufacturers, software developers, and product security teams will walk away with new insights into how to improve the resilience of medical devices against cyberattacks.

Medical Device Software at Risk

Specialized medical devices, including pacemakers, ventilators, and diagnostic imaging machines, enhance healthcare delivery by enabling real-time monitoring and diagnosis. For example, pacemakers can send alerts to remote physicians about heart irregularities, allowing for prompt life-saving interventions. In another example, robotic systems are increasingly used for surgeries, with human surgeons overseeing operations from miles away.

Unfortunately, many of these devices are vulnerable to cyberattacks due to vulnerabilities in the underlying software. Vulnerabilities such as memory unsafe software, weak encryption, and insecure communication protocols make these devices attractive targets for cybercriminals seeking to exploit their weaknesses. As these risks continue to grow, the security of embedded medical devices must become a top priority in the healthcare sector.

In 2011, frustrated by a lack of vendor support for the vulnerabilities he had discovered, researcher Jay Radcliff hacked his own insulin pump live on stage at Black Hat USA. He successfully jammed the wireless signal between his external monitor and the implant in his body, creating a temporary denial of service. Following the demonstration, the unnamed vendor collaborated with Radcliff to enhance the product's security.

In 2013, researcher Barnaby Jack showcased his ability to manipulate the signal of a wireless defibrillator from over 100 feet away. This raised serious concerns about the security of medical devices. In fact, when former Vice President Dick Cheney had his implanted defibrillator replaced in 2007, his cardiologist requested the manufacturer to disable its remote access feature due to fears that terrorists could exploit it to disrupt its function.

Similarly, in 2015, students at the University of Washington demonstrated a remote takeover of robotic surgical equipment using public telecommunications. While surgical devices approved for clinical use rely on private telecommunication channels, they may still share communication protocols similar to those identified in the research, highlighting potential security risks in connected medical technologies.

Key risks of a successful attack include:

Compromised Patient Data: One of the most critical risks is the exposure of sensitive patient information. Medical records contain personal data such as medical histories, treatment plans, and insurance details. In the wrong hands, this information can be exploited for identity theft, insurance fraud, or sold on the dark web. Breaches of patient data not only violate privacy laws like the Health Insurance Portability and Accountability Act (HIPAA), they also damage the trust patients place in healthcare providers.

Interference with Device Functionality: Beyond data breaches, cyberattacks can disrupt the operation of medical devices, potentially endangering patient lives. A cybercriminal could manipulate the settings of devices such as a pacemaker or diagnostic machine, leading to dangerous situations where patients receive incorrect care or suffer from critical device malfunctions. Even minor tampering with software could result in faulty readings or incorrect diagnoses, directly impacting treatment outcomes.

Patient Safety: The most serious consequence of a cyberattack is the direct threat to patient safety. In extreme cases, a hacker could take control of life-sustaining devices like ventilators, MRI machines, or cardiac monitors, intentionally causing harm. Additionally, widespread attacks on hospital networks that disrupt multiple devices simultaneously could overwhelm healthcare staff and delay urgent medical care.

In this context, securing medical devices is not only about protecting data but also about safeguarding patient lives and ensuring the reliable operation of critical medical devices.

Regulatory Oversight

Because of the risks, governments and international regulatory bodies have begun to issue guidelines and standards MDMs must comply with across every stage of a device's development lifecycle.

Key aspects of these regulations include:

- **Physical design and functionality:** Ensuring devices meet rigorous performance and safety standards.
- **Cybersecurity and software integrity:** Addressing the growing integration of technology in healthcare and mitigating risks associated with data breaches or software vulnerabilities.

For manufacturers, a thorough understanding of these regulatory requirements is essential to:

- **Ensure compliance:** Avoid penalties or delays in bringing products to market.
- **Maintain market access:** Adhere to global standards to remain competitive across international markets.
- **Protect patient safety:** Proactively address risks to enhance device reliability and health outcomes.

Key Medical Device Regulations

FDA Cybersecurity Guidance

The U.S. Food and Drug Administration (FDA) has issued comprehensive guidance on medical device cybersecurity, emphasizing premarket and postmarket considerations. Key takeaways include recommendations for device labeling, risk assessments, and the implementation of security controls.

The guidelines focus on a total product lifecycle (TPLC) approach that maps out the entire software development lifecycle—from design through post-release. These guidelines include clear definitions of the device's end-of-support phase and mandate that manufacturers create a comprehensive cybersecurity risk management plan. This plan should detail how they will identify, assess, and mitigate cybersecurity risks throughout the device's lifecycle.

Manufacturers must also document their processes for addressing vulnerabilities — after market release — ensuring that protocols are in place for timely updates and user notifications regarding security risks. This proactive strategy is essential for protecting patient safety and maintaining the integrity of medical devices in an increasingly interconnected healthcare landscape. Recently, the FDA acknowledged three new international standards related to software security in medical devices, highlighting the significance of this issue.

EU MDR/IVD

The European Union's Medical Devices Regulation (MDR) and In Vitro Diagnostic Medical Devices Regulation (IVDR) mark a significant transformation in the regulation of medical devices, aiming to bolster patient safety and optimize device performance across European markets. These regulations introduce stricter requirements for clinical evidence, robust post-market surveillance, and a lifecycle-focused approach to device management. Manufacturers are now tasked with achieving higher levels of transparency, traceability, and consistent quality monitoring.

Key changes include the implementation of mandatory unique device identification (UDI), more rigorous clinical evaluation processes, enhanced documentation standards, and comprehensive risk management strategies. Companies must provide detailed clinical data, establish advanced quality management systems, and maintain proactive post-market surveillance to ensure ongoing compliance. Together, these reforms are reshaping how medical devices are designed, validated, and monitored throughout their lifecycle in the European Union, setting a new standard for safety and accountability.

ANSI and AAMI Guidance

One standard, developed by the American National Standards Institute (ANSI) and the Association for the Advancement of Medical Instrumentation (AAMI), is ANSI/AAMI 2700-2-1. This standard is part of a broader set aimed at ensuring the safe use of medical device software in integrated clinical environments (ICE) and focuses on the effectiveness of data loggers in these systems for supporting improvements and updates.

The second standard, ANSI AAMI SW96:2023, establishes requirements for managing security risks associated with medical devices. It guides manufacturers in adopting a Total Product Life Cycle (TPLC) approach to managing devices that incorporate software with potential cybersecurity vulnerabilities. This document outlines various aspects that can enhance the security of medical devices, including threat identification, vulnerability assessment, and appropriate risk mitigation controls.

IEC 62304 and ISO 14971 Standards

IEC 62304 focuses on the safe design and maintenance of medical device software, while ISO 14971 provides a framework for identifying risks and implementing controls throughout the device lifecycle. Combining these standards establishes a strong foundation for software security.

The Medical Device and Health IT Joint Security Plan (JSP)

The JSP serves as a voluntary framework designed to assist medical device manufacturers and healthcare IT providers in assessing, prioritizing, and enhancing their product security programs. Additionally, the Model Contract Language for Medtech Cybersecurity offers a template and maturity model for establishing cybersecurity contract terms between healthcare delivery organizations and medical device manufacturers.

Secure Development Practices for Medical Devices

To enhance the security of medical device software, manufacturers should consider the following strategies.

Adopt a Secure Product Development Framework (SPDF)

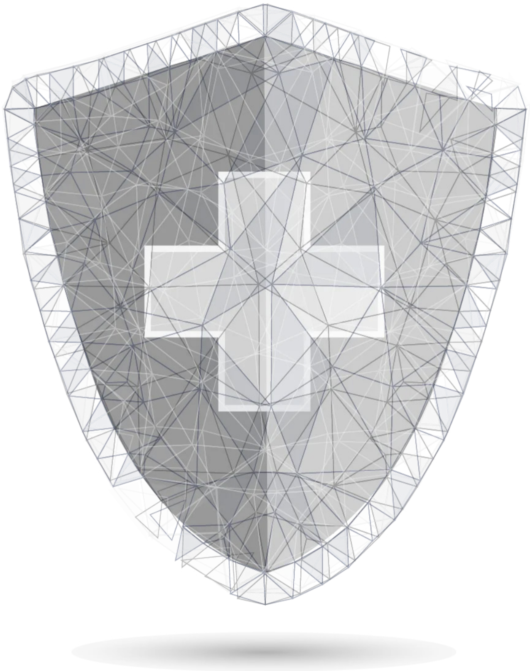
A Secure Product Development Framework (SPDF) ensures that security is a priority throughout the entire software development lifecycle. This structured approach integrates security considerations from the early stages of design to deployment and maintenance. For medical devices, aligning with standards like IEC 81001-5-1:2021 is vital, as it focuses on security for health software and health IT systems, ensuring that devices meet industry regulations and reduce vulnerabilities.

Follow Established Coding Standards

Coding standards like MISRA and CERT provide essential guidelines to improve software security and quality. By adhering to these standards, developers can mitigate common vulnerabilities and write safer, more reliable code. Additionally, industry-specific standards like IEC 62304, which focuses on medical device software lifecycle processes, help ensure that the development process is both safe and compliant.

Implement "Secure by Design and Default" (SBDD) Principles

Building security into the design of a medical device from the start minimizes vulnerabilities and reduces the likelihood of security breaches. "Secure by Design and Default" principles emphasize creating solutions with security features as a baseline, rather than adding them as an afterthought. By integrating these principles at every stage of development, manufacturers can significantly reduce the attack surface of their devices.



Conduct Thorough Risk Management

Risk management is an essential part of any secure development practice. Using ISO 14971, medical device manufacturers can systematically identify and manage risks, including cybersecurity threats. Continuous security evaluations at each development phase ensure that new vulnerabilities introduced during the process are quickly identified and addressed, minimizing risks to end users.

Implement Vulnerability Management Processes

An effective vulnerability management process is essential for maintaining secure medical devices over time. This involves regularly identifying, assessing, and addressing vulnerabilities in both proprietary software and third-party components. By implementing timely patching, updates, and continuous monitoring, manufacturers can reduce risks, ensure compliance with regulatory standards, and prioritize patient safety and data security.

Ensure Regulatory Compliance

Regulatory compliance is non-negotiable in the medical device industry. Following FDA and ISO guidelines for cybersecurity ensures that devices meet strict safety and security requirements. Manufacturers should establish processes to identify security risks, implement appropriate controls, and document their efforts to align with regulatory standards.

Code Review and Static Analysis

Regular peer code reviews and the use of static analysis tools are essential for identifying and addressing security flaws early in the development process. Peer reviews allow developers to cross-check for mistakes, while static analysis tools automatically scan code for vulnerabilities, ensuring critical bugs are caught before deployment.

Implement Input Validation

Input validation is a critical measure for preventing common attack vectors like injection attacks and buffer overflows. All user inputs should be thoroughly validated and sanitized to ensure they meet expected formats and values. This simple yet effective step can prevent many common cybersecurity threats from exploiting vulnerabilities in the system.

Maintain a Software Bill of Materials (SBOM)

A Software Bill of Materials (SBOM) provides a detailed inventory of all software components used within a medical device. Maintaining an up-to-date SBOM allows manufacturers to quickly identify and address vulnerabilities as they arise. Regular vulnerability scanning ensures that devices remain secure throughout their lifecycle.

A Focus on Software Bill of Materials (SBOMs)

In the medical device industry, software plays a key role in device functionality and patient safety. An SBOM enhances transparency and compliance by providing a comprehensive inventory of all software components used in a device. This visibility is crucial for manufacturers, healthcare providers, and regulators to ensure that devices meet safety and performance standards.

Regulatory Requirements for SBOMs

Regulatory bodies worldwide are increasingly recognizing the importance of SBOMs in ensuring the security and safety of medical devices. For example, the U.S. Food and Drug Administration (FDA) has issued guidance emphasizing the role of SBOMs in premarket submissions for cybersecurity preparedness. The FDA recommends that manufacturers include an SBOM in their device documentation to provide visibility into software supply chains and address potential vulnerabilities. Similarly, global standards like IEC 62304 focus on software lifecycle processes, encouraging manufacturers to maintain detailed documentation of software components, which aligns closely with the purpose of an SBOM. These requirements underscore the importance of maintaining up-to-date SBOMs for regulatory compliance and market approval.

SBOM Generation and Vulnerability Identification

Creating and maintaining an SBOM is not a one-time task; it requires regular updates to reflect the latest software configurations and any changes made during the lifecycle of the device. This dynamic approach ensures that manufacturers have a current and accurate view of the software components, which is essential for addressing vulnerabilities promptly and for demonstrating compliance with regulatory standards.

Within the medical device industry, generating comprehensive SBOMs is often a challenge as many embedded devices are written in C/C++. Common solutions, like binary analysis, are not able to capture all software components accurately, leading to a high number of false positives for developers to chase.

Medical device manufacturers should consider build-time SBOM solutions that provide an accurate picture of software by capturing only the components and libraries that are actually in a build. By doing so, manufacturers can stop investigating vulnerabilities that will not be in the final build, streamlining vulnerability identification and increasing the resilience of embedded systems.

SBOMs enable manufacturers to quickly assess which components may be impacted by newly discovered vulnerabilities and take swift action to patch or update them. This is particularly vital in the medical device industry, where cybersecurity risks can directly affect patient safety.

Applying SBOMs Post-Market

Beyond regulatory compliance, SBOMs play a key role in the manufacturing and post-market management of medical devices. During the manufacturing process, SBOMs help manufacturers maintain quality control and ensure that only approved software components are integrated into devices. Post-market, SBOMs provide a foundation for ongoing maintenance, allowing device manufacturers to respond quickly to cybersecurity threats or software compatibility issues. In an era where cyberattacks on healthcare infrastructure are on the rise, having a robust SBOM process in place is no longer optional—it's a necessity.

Lifecycle Management

Medical device software security demands a comprehensive, ongoing approach that spans the entire product lifecycle. This section outlines key strategies for security throughout the development, deployment, and maintenance of medical device software.

Secure by Design: A Lifecycle Approach

Integrating security at every stage of a medical device's lifecycle is crucial for long-term protection and regulatory compliance. This proactive approach not only mitigates vulnerabilities early but also significantly reduces the risk of costly issues in later stages.

Development Phase

During the development phase, manufacturers must:

- Conduct thorough threat assessments
- Carefully select secure components
- Implement robust security controls
- Create comprehensive documentation on the device's security posture

For instance, implementing secure coding practices and conducting regular code reviews can help identify and address potential vulnerabilities before they become critical issues.

Support Phase

As devices enter the market, the focus shifts to:

- Providing regular updates for clinical functionality and user experience
- Issuing timely security patches
- Maintaining clear communication channels with healthcare delivery organizations (HDOs)

Example: A pacemaker manufacturer might release quarterly firmware updates to address newly discovered vulnerabilities, ensuring the device remains secure against evolving threats.

Post-Market Surveillance: Vigilance in Action

Post-market surveillance is a critical component of the medical device lifecycle, allowing manufacturers to monitor device performance and security in real-world settings.

Key aspects include:

- Systematic collection and analysis of user feedback and incident reports
- Continuous monitoring of cybersecurity threats and vulnerabilities
- Regular risk assessments, especially as devices approach end-of-life (EOL) or end-of-support (EOS) stages

For example, a medical imaging software company might deploy runtime exploit prevention to defend devices, including legacy devices, post-market.

Vulnerability Disclosure

Implement a transparent vulnerability disclosure policy that:

- Encourages responsible reporting of potential security issues
- Outlines a clear process for addressing and resolving reported vulnerabilities
- Demonstrates commitment to ongoing security improvement

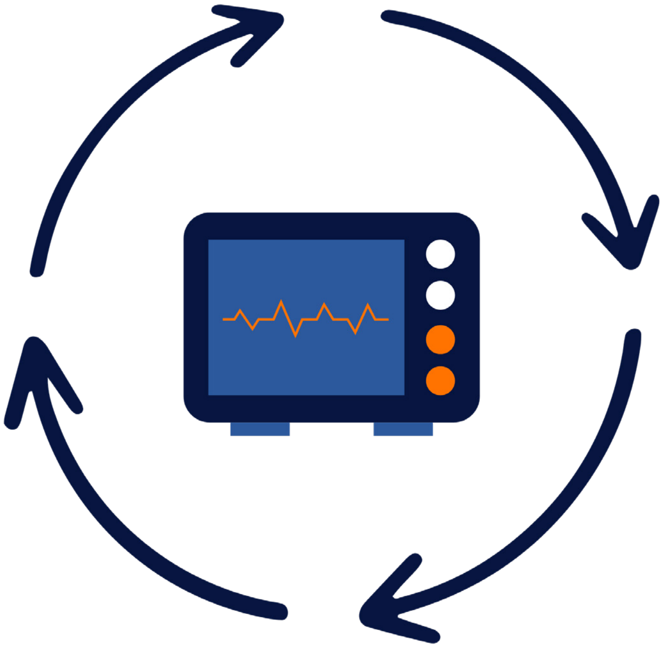
Example: A medical device manufacturer might partner with cybersecurity researchers through a bug bounty program, offering incentives for responsibly disclosing vulnerabilities and collaborating on fixes.

Leveraging Software Bill of Materials (SBOM)

Incorporating SBOM practices throughout the device lifecycle enhances transparency and security management:

- During development: Collect and document SBOM content for all software components
- In support phase: Regularly update and distribute SBOM information to stakeholders
- For vulnerability management: Use SBOM to quickly identify affected devices when new vulnerabilities are discovered

By maintaining accurate SBOM records, manufacturers can rapidly assess the impact of newly discovered vulnerabilities and prioritize patching efforts effectively.



Security Protections for Medical Device Software

Securing medical devices is a critical challenge, especially when addressing vulnerabilities that require timely patching. However, immediate updates aren't always feasible due to the complexities of healthcare environments and the logistics of deploying patches to devices in the field.

This is where runtime exploit prevention offers a game-changing solution for medical device software security. Acting as a built-in self-defense mechanism, runtime protections safeguard devices from sophisticated malware, unauthorized code execution, hidden backdoors, and unknown vulnerabilities, even before a patch becomes available.

By integrating runtime exploit prevention directly into device software, manufacturers can significantly reduce the risk of exploitation. If an attacker targets a vulnerability, the technology enables the device to defend itself in real time, preventing critical attacks while maintaining patient safety.

While patches remain essential for long-term security, runtime protections buy valuable time, ensuring devices remain secure and functional in situations where immediate updates aren't possible. For medical device manufacturers and healthcare providers, this proactive approach is a vital layer of defense in an increasingly complex threat landscape.

Example Case Studies of Medical Devices Protected by RunSafe

1. **Accelerating Time to FDA Approval:** A medical device company was seeking a way to accelerate its time to FDA approval by dramatically reducing its attack surface and minimizing the severity of vulnerabilities so it can optimize its scanning, fixing, and patching processes. With RunSafe's runtime exploit prevention solution, the company's devices are protected from exploitation for both known and unknown vulnerabilities.

2. **Addressing Software Supply Chain Risk:** One product security team leveraged the RunSafe Security Platform for embedded developers to extend its return on investment by rolling out a centralized way to generate SBOMs, identify vulnerabilities, and integrate vulnerability mitigation within its build tools.

3. **Securing IoT Medical Devices:** By implementing runtime exploit prevention, RunSafe fortifies IoT medical devices against common malware attacks, memory corruption errors, buffer overflows, and zero-day exploits, ensuring continuous and safe operation.

Benefits of Proactive Security

Strengthen Premarket Submissions: Runtime exploit prevention shows manufacturers are proactively securing devices, reducing risks from vulnerabilities and zero days and eliminating the timeframe from vulnerability disclosure to patch that leaves devices open to exploit.

Streamlined Patching: Runtime protection allows manufacturers to delay patches without compromising security, aligning updates with planned upgrades to minimize disruptions.

Fewer FDA Re-approvals: Reducing patch frequency means fewer costly and time-consuming FDA re-approvals.

Improved Device Resilience: Runtime protections defend medical devices throughout their lifespan, strengthening device security and healthcare system resilience over time.

Conclusion: Securing the Future of Medical Device Software

The increasing complexity of medical technology demands a comprehensive, proactive approach to cybersecurity. As we have explored throughout this white paper, medical device software security is no longer an optional consideration—it is a critical imperative that directly impacts patient safety, data protection, and healthcare system integrity.

Key takeaways include:

1. **Holistic Security Strategy:** Medical device manufacturers must adopt a “Secure by Design and Default” approach, integrating security considerations from the earliest stages of development through the entire device lifecycle.
2. **Regulatory Compliance:** Staying current with evolving regulations from the FDA, ANSI, AAMI, and international bodies is crucial. These guidelines provide essential frameworks for managing cybersecurity risks and protecting patient well-being.
3. **Continuous Vigilance:** Security is not a one-time achievement but an ongoing process. Regular risk assessments, vulnerability management, and post-market surveillance are essential to maintaining device resilience.
4. **Advanced Protection Mechanisms:** Technologies like runtime exploit prevention offer promising solutions for defending medical devices against sophisticated cyber threats, providing an additional layer of security that can protect devices even before patches are available.
5. **Transparency and Collaboration:** Maintaining comprehensive Software Bills of Materials (SBOMs) and establishing clear vulnerability disclosure policies will foster trust and enable rapid response to emerging security challenges.

Looking ahead, the medical device industry must continue to innovate, prioritizing security as a fundamental aspect of device design and functionality. As healthcare becomes increasingly digital and interconnected, the stakes for cybersecurity have never been higher. By embracing a proactive, collaborative approach to software security, manufacturers can ensure that technological advancements enhance—rather than compromise—patient care.

RUNSAFE
SECURITY

ABOUT RUNSAFE SECURITY, INC.

RunSafe Security is the pioneer of a unique cyberhardening technology designed to disrupt attackers and protect vulnerable embedded systems and devices. With the ability to make each device functionally identical but logically unique, RunSafe Security renders threats inert by eliminating attack vectors, significantly reducing vulnerabilities, and denying malware the uniformity required to propagate. Based in McLean, Virginia, with an office in Huntsville, Alabama, RunSafe Security's customers span the Industrial Internet of Things (IIoT), critical infrastructure, automotive, and national security industries.

www.RunSafeSecurity.com

571.441.5076

sales@RunSafeSecurity.com