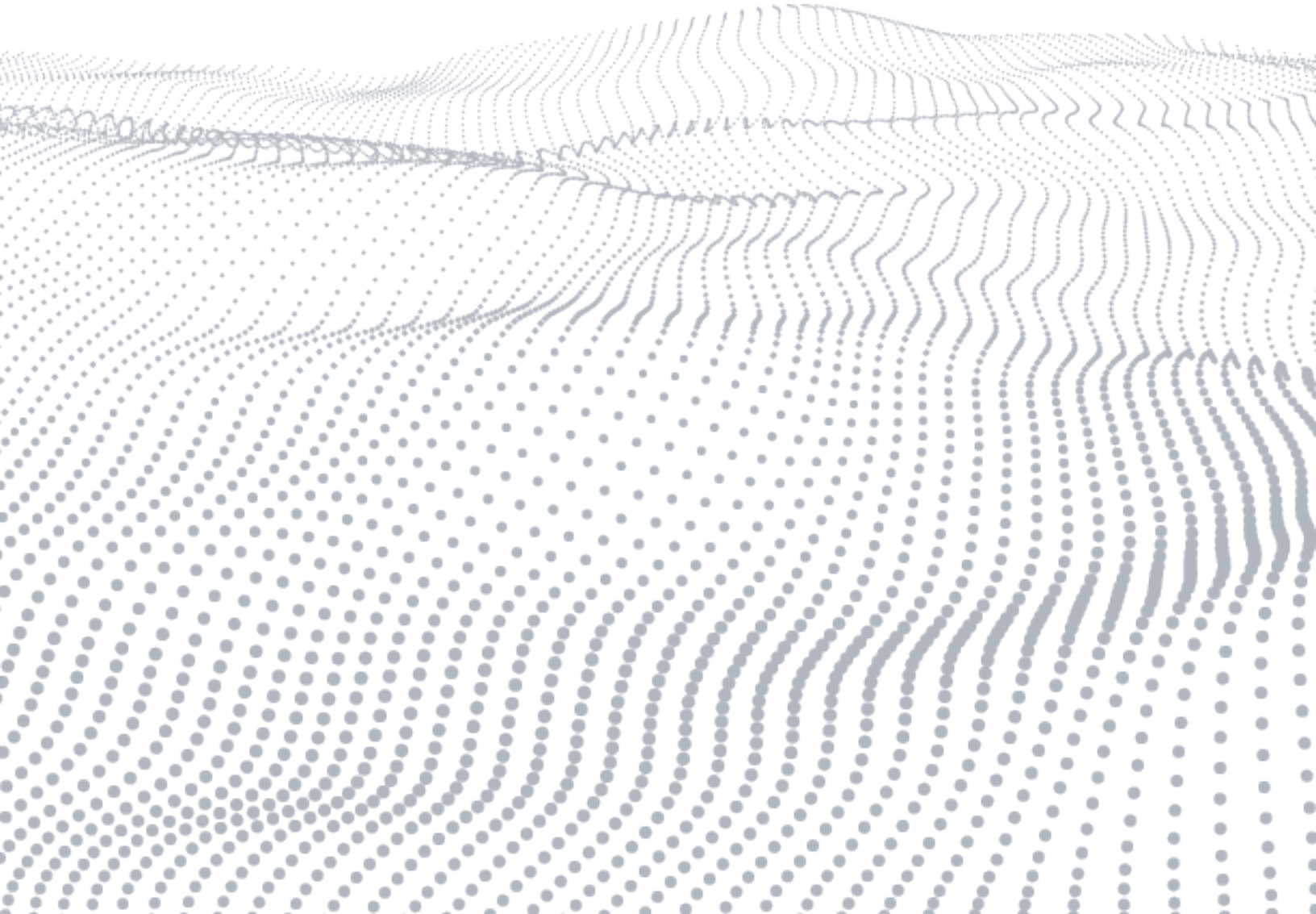
BLACKDUCK®

WHITE PAPER

Securing Connected Medical Devices for FDA Submissions



Medical device security and regulatory landscape

The Internet of Things (IoT) is transforming entire industries while bringing tremendous freedom, benefits, and opportunities to consumers and businesses alike. However, it also introduces new software application security (AppSec) and safety risks that are compounded by the need to get devices to market as quickly as possible. The benefits and challenges of the IoT are especially evident in healthcare, thanks to increases in the volume and use of medical devices.

This paper investigates the security and regulatory landscape, especially as it relates to the U.S. Food and Drug Administration (FDA), and it provides best practices for medical device manufacturers and healthcare delivery organizations looking to achieve and maintain FDA regulatory compliance.

Increasing interconnectedness of medical devices

Network-connected medical devices have helped improve patient care. Hospital imaging equipment, pacemakers, and infusion pumps, just to name a few, help healthcare providers monitor vital signs, regulate medication dosages, improve diagnostics, and deliver therapies that ultimately improve patient outcomes while lowering costs.

The use and sophistication of software in medical devices have increased exponentially since the early 2000s, when Vitatron (now Medtronic) introduced the first digital pacemaker.[1] Initially, the software was composed entirely of custom code written from scratch; however, software soon became componentized and sourced from both commercial parties and open source communities. Frameworks, libraries, and "copy and paste" code are now linked in a complex web of dependencies that enable fast development to keep up with demand. But as a result, development teams are not fully aware of all the dependencies in their software.

As technologies such as big data, artificial intelligence, and machine learning become increasingly prevalent, software will be even more essential to the next generation of life-sustaining therapies. This has already been seen during the COVID-19 pandemic, as telehealth became a viable treatment path that provides greater access and convenience. Its use has increased 38 times since pre-COVID-19 baselines.[2]

The COVID-19 pandemic has also increased the number of medical devices used at home. The FDA issued emergency use authorizations for certain wearable patient devices to help increase the availability of patient monitoring and treatment, as well as to reduce healthcare provider exposure to SARS-CoV-2.[3]

Medical device security, safety, and regulatory risks

With access to so much personal data, medical devices have become a popular and profitable target for hackers and other bad actors. At the same time, the increasing complexity and interconnectedness of such devices have made them more susceptible to attacks. Fraud, supply chain disruptions, stock manipulation, ransomware, and theft of identities, proprietary information, and research and development data have all been linked to cyber attacks on medical devices. There is also the threat of disrupted patient care with serious health consequences, including loss of life.

Manufacturers and healthcare delivery organizations must address the security, safety, and regulatory risks of connected devices if they are to be fully trusted by doctors, patients, governments, and society at large.

Security risks

As mentioned, the COVID-19 pandemic has brought a sharp increase in the use of medical devices such as CT scanners, monitoring systems, patient telemetry systems, and ventilators. Because such devices are being used more, attacks on them are increasing. One report shows a 42% increase in hacking incidents of medical devices during the first year of the pandemic.[4]

Vulnerabilities in medical devices existed well before COVID-19. In 2019, there was an average of 6.2 vulnerabilities per medical device.[5]

A report by the Ponemon Institute,[6] commissioned by Black Duck, found that:

- 60% of medical device manufacturers and 49% of healthcare delivery organizations report that using mobile devices in hospitals and other sites significantly increases security risks
- 53% of medical device manufacturers say there is a lack of quality assurance and testing procedures
- 43% of medical device manufacturers either don't test or aren't sure if they test medical devices at least once per year
- 37% of medical device manufacturers believe they can detect security vulnerabilities in their devices
- 33% of medical device manufacturers say they encrypt traffic among IoT devices; of these, only 39% use key management systems on encrypted traffic

According to research and advisory firm Forrester,[7] medical devices are vulnerable to four attack scenarios:

- Denial of service (DoS)
- Therapy manipulation
- Patient data theft
- Asset damage

Ransomware attacks and security breaches

Ransomware attacks attempt to extort the target, and in doing so they can disrupt patient therapies. When clinics and hospitals cannot access data and critical systems, patient lives are at risk. This also causes financial harm to the healthcare delivery organization due to decreased quality and level of care.

Recent ransomware attacks in healthcare include:

- May 2021, an attack on the Scripps Health network and encrypted devices resulted in a data breach, loss of access to electronic medical records, the diversion of trauma and stroke cases to other hospitals, and class-action lawsuits[8]
- May 2021, an attack disabled the Irish Healthcare Service, cutting off access to patient records, delaying COVID-19 testing, forcing appointment cancellations, and compromising the sending, receiving, and comparing of scans from medical imaging devices; the attackers demanded $20 million in Bitcoin,[9] and the same ransomware targeted at least 16 medical and emergency networks in the U.S.[10]
- April 2021, an attack of 42 U.S. healthcare sites disrupted the cloud services necessary for critical function of cancer radiation therapy[11]

Recalls

According to the Ponemon Institute, 24% of medical device manufacturers and 19% of healthcare delivery organizations had recalled a device because of security vulnerabilities as of May 2017.[12] Since then, the U.S. Food and Drug Administration (FDA) has reported many more recalls impacting hundreds of millions individual devices.[13]

Safety risks

Patient lives often rely on pacemakers, insulin pumps, dialysis machines, and other devices to augment organs or control vital body functions. Any failure in such devices can have severe consequences for patients, including illness, injury, disability, and death. This harm may stem from device performance or malfunctions, impeded hospital operations, or the inability to deliver care.

Safety risks posed by cyber threats include:

- Malware altering data on a diagnostic device
- Reprogramming of a device that alters function
- Denial of service attacks that render a device unavailable
- Unauthorized network access that makes other devices vulnerable
- Uncontrolled passwords

Each year, the FDA receives several hundred thousand medical device reports (MDRs) of suspected device-associated deaths, injuries, and malfunctions. The reports are published in the publicly available database, Manufacturer and User Facility Device Experience (MAUDE). Additionally, in June 2019, the FDA released approximately 6 million reports filed by manufacturers relating to medical device malfunctions that occurred between 1999 and 2019 that were not included in MAUDE.[14]

Regulatory risks

Medical device manufacturers must ensure that devices and applications meet patient expectations and comply with regulations. Manufacturers must understand the legal ramifications of enforcement actions, especially product recalls, and think holistically about the risks and exposure associated with state and international laws, rules, statutes, and litigation.

Regulation of medical device cyber security

Increased government oversight has led to the rapid adoption of AppSec solutions in the healthcare sector, including for medical devices. Laws and regulations addressing the security and safety risks of medical devices include:

- **Federal Food, Drug, and Cosmetic (FD&C) Act of 1938:** Section 501(f), Section 515, and Section 510(k) for U.S. medical devices (21 CFR 807); Medical Device Amendments of 1976
- **Safe Medical Devices Act (SMDA) of 1990**
- **Health Insurance Portability and Accountability Act (HIPAA) of 1996**
- **Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009**
- **European Union medical devices regulation (MDR) 2017/745**

A variety of public and private sector organizations—including the FDA, the National Institute of Standards and Technology (NIST), Association for the Advancement of Medical Instrumentation (AAMI), International Electrotechnical Commission (IEC), and American National Standards Institute (ANSI)—have developed guidance and standards to help medical device manufacturers comply with applicable laws and regulations.

General standards for medical device security include:

- AAMI TIR57: Principles for medical device security—risk management
- AAMI TIR97: Principles for medical device security—postmarket risk management for device manufacturers
- AAMI draft standard SW96: Medical devices—application of security risk management to medical devices
- IEC 62304: Medical device software—software life cycle processes
- IEC/ANSI/ISA 62443-4-1: Security for industrial automation and control systems—secure product development life cycle requirements

The sheer number and complexity of regulations, standards, and recommendations make it difficult for organizations to maintain compliance. For instance, for medical devices marketed in the U.S., manufacturers must undertake the FDA premarket notification 510(k) and/or premarket approval process, in addition to meeting any other specific standard that requires compliance.

Medical device manufacturers need AppSec solutions to help them identify security risks in their software, balance those risks with device usability and availability, and achieve and maintain regulatory approval.

FDA cyber security risk management considerations

The U.S. government has charged the FDA with ensuring that medical devices are safe and effective. It limits FDA oversight to patient safety and doesn't extend to patient privacy. Since 2005, the FDA Center for Devices and Radiological Health (CDRH) has undertaken several initiatives to advise manufacturers on designing and developing medical devices that are safe and secure.

Medical device classification levels

The FDA classifies medical devices based on their intended use, indications for their use, and the risk they pose to the patient or user. The intended uses of medical devices range from simple thermometers to devices connected to the internet to help with medical testing, implants, and prostheses. Software is used in a variety of contexts including robots, implantable devices, wearable devices, equipment like MRIs and CT scans, diagnostic and monitoring equipment, networking equipment designed specifically for medical devices, and mobile medical applications.

The FDA has three classes of medical devices:

- **Class I devices** pose low risk to patient safety and include Bluetooth-enabled toothbrushes, hospital beds, and monitored surgical instruments. Almost half (47%) of all medical devices fall under this category, and 95% of them are exempt from the regulatory process.[15]

- **Class II devices** pose moderate risk to patient safety and include infusion pumps, wearable devices such as the Apple Watch, and equipment like MRIs and CT scans; 43% of medical devices fall under this category.[16]
- **Class III devices** pose high risk to patient safety and are subject to stringent regulatory controls. These devices include pacemakers, cerebellar stimulators, and insulin and other medication pumps with invasive glucose sensors. Only 10% of medical devices fall under this category.[17]

In 2018, the FDA drafted premarket guidance that introduced a two-tier classifications system based specifically on the cyber security risk of medical devices:

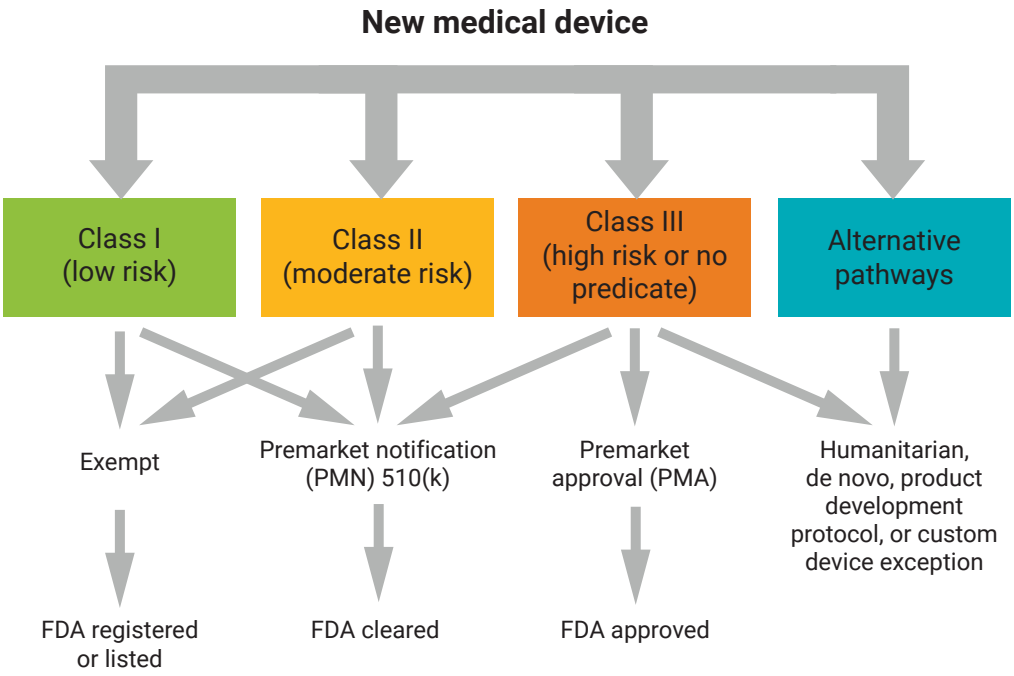
- **Tier 1 devices** pose high cyber security risk
- **Tier 2 devices** pose standard cyber security risk

The FDA recognizes these tiers may not match its existing statutory device classifications, further complicating the challenge that manufacturers have in achieving FDA compliance.

Clearance and approval

Before marketing a medical device in the U.S., the submitter must receive clearance from the FDA in the form of an order letter that states the FDA finds the device to be substantially equivalent to a legally marketed device.

The class of the medical device determines the type of premarket submission or application required for FDA clearance to market the device (see graphic below). Regardless of class, any device that isn't exempt requires clearance. Class III devices as well as devices that are completely new to the market require an additional and more stringent premarket approval (PMA).



FDA requirements for new medical devices marketed in the U.S.

Premarket notification 510(k)

Section 510(k) of the FD&C Act (often referred to as a premarket notification 510(k) or PMN 501(k)) represents the clearance process a medical device must complete prior to going to market in the U.S. It involves a submission made to the FDA to demonstrate the device is as safe and effective as an existing device that is legally marketed.

Manufacturers must submit a PMN 501(k) if they intend to introduce a device into commercial distribution for the first time or reintroduce a significantly modified device.

Premarket approval

Class III devices require a PMA application in addition to a Class III PMN 510(k) to obtain FDA approval. If a Class III device fails to meet PMA requirements, the FDA considers it adulterated and it cannot be marketed in the U.S.

FDA guidance

In addition to regulatory oversight, the FDA issues premarket and postmarket guidance for medical device cyber security and risk management. This guidance is issued in the form of documents published by the FDA CDRH.

While FDA guidance is nonbinding and not requirements, it provides rationale and details behind its recommendations, which align with the NIST Cyber Security Framework. While the guidance is not legally enforceable, some organizations choose to adopt the recommendations and make them requirements of their own accord. By referencing FDA guidance documents, these organizations are better prepared to submit a PMN 501(k) or PMA that attests how they have complied with the requirements.

Premarket guidance

FDA premarket guidance focuses primarily on helping organizations with the PMN 501(k) and/or PMA submission process. In general, medical device manufacturers should:

- Develop a set of controls to assure cyber security and maintain device functionality and safety
- Address cyber security during the design and development of medical devices

Potential new premarket requirements are being outlined by the FDA, the Department of Health and Human Services, and Congress. They would require organizations to take steps on medical device security, software updates, and a software Bill of Materials (SBOM). They also propose that medical device safety would be advanced if the FDA requires manufacturers to:

- Update and patch devices in a timely manner
- Include evidence in FDA premarket submissions that demonstrates the capability of device updating and patching from a design and architecture perspective
- Use a phased-in approach for a cyber security Bill of Materials (CBOM) or SBOM
- Publicly disclose known cyber security vulnerabilities in their devices and provide direction to customers on reducing their risk
- Improve proactive responses to cyber security vulnerabilities

In 2018, the FDA revised its premarket guidance document to address these proposals, recommending that security become a design input in the development process of medical devices along with safety. And the FDA requires manufacturers to submit a 510(k) PMN or PMA based on the 2018 updates.

The FDA intends for the updated guidance to help manufacturers:

- Employ a risk-based approach to the design and development of medical devices with appropriate security protections
- Take a holistic approach to device cyber security by assessing risks and mitigations throughout a device's life cycle
- Ensure the maintenance and continuity of a device's critical safety and essential performance
- Promote the development of trustworthy devices to help ensure continued safety and effectiveness

Integrating security into design and development

The FDA premarket guidance describes designing a trustworthy device using a life cycle that addresses security at every step of the process. It recommends establishing design inputs for device development that:

- Identify assets, threats, and vulnerabilities
- Assess the impact of threats and vulnerabilities on device functionality and on end users/patients
- Assess the likelihood of an attacker exploiting a threat or vulnerability
- Determine the risk levels and suitable mitigation strategies
- Assess residual risk and acceptance criteria

Security controls

The premarket guidance provides example security controls for limiting access to trusted users, ensuring trusted content, and detecting, responding to, and recovering from security compromises. Manufacturers should identify and evaluate all controls through risk assessments.

Device intended use

The FDA recommends that manufacturers balance cyber security safeguards with the usability of a device in its intended environment so that security controls are appropriately employed. Manufacturers should document the rationale behind these considerations to justify the security functions used (and not used) as part of their premarket submissions.

Labeling recommendations

The FDA premarket guidance includes the concept of providing a CBOM to help identify assets, threats, and liabilities. A CBOM helps manufacturers understand exposure to risk of both known and future vulnerabilities in third-party software of legacy devices. This labeling targets end users, IT personnel, and other support staff responsible for integrating the device into existing infrastructure.

End-of-life instructions are critical to help customers to understand the increasing risks once the manufacturer no longer supports a device.

Documentation

The FDA provides a list of cyber security topics that the manufacturer should discuss and document as part of its premarket submissions. These topics include design, system diagrams, a system threat model, and risk management documentation.

Postmarket guidance

Focusing on cyber security after medical devices are deployed, the FDA's postmarket guidance is more substantial than its premarket guidance. Postmarket, the FDA "emphasizes that manufacturers should monitor, identify, and address cyber security vulnerabilities and exploits as part of their postmarket management of medical devices."[18]

Integrating security throughout the product life cycle

One of the key principles discussed in the FDA postmarket guidance document is the implementation of security by design throughout the product life cycle, including operations and maintenance. "An effective cyber security risk management program should incorporate both premarket and postmarket life cycle phases and address cyber security from medical device conception to obsolescence."[19]

This guidance reflects the industry best practice of designing and building security in from the very beginning and continuing to address it until a product is retired. Postmarket guidance also stresses the importance of testing medical devices against vulnerabilities throughout its life cycle, including in the manufacturer's proprietary code, third-party code, and hardware.

FDA postmarket guidance includes how to assess the impact of vulnerabilities to determine risks to patients (the FDA's primary focus); however, it doesn't address risks to a manufacturer's business, revenue, reputation, or other considerations.

Threat modeling

The FDA promotes the importance of an up-to-date threat model to help assess the possible impact of threats. It also suggests that manufacturers assess vulnerabilities even if they don't present a current risk but may in the future. It recommends using tools such as the Common Vulnerability Scoring System to provide consistency to the risk assessment process.

Information sharing

The FDA advises monitoring a variety of sources for cyber security vulnerabilities and risks, to assess them against a manufacturer's devices. It suggests participation in information-sharing organizations in which members share vulnerability data, so manufacturers can assess their own exposure. It specifically lists the Health Information Sharing and Analysis Center (Health-ISAC or H-ISAC) as one such organization.

The FDA also suggests a coordinated vulnerability disclosure policy and practice to manage activities across the organization and with customers.

Vulnerability reporting

The FDA provides guidance and sets thresholds on remediation timelines for how quickly to respond to reported vulnerabilities. Recommended actions include communicating to customers, providing workarounds and mitigation information, and developing and deploying fixes. This guidance is in response to the failure of manufacturers to promptly address vulnerabilities according to industry standards and best practices.

Uncontrolled risks

FDA postmarket guidance also discusses a situation in which a medical device presents uncontrolled risk. "In the absence of remediation, a device with uncontrolled risk of patient harm may be considered to have a reasonable probability that use of, or exposure to, the product will cause serious adverse health consequences or death. The product may be considered in violation of the FD&C Act and subject to enforcement or other action."[20]

Challenges of FDA cyber security compliance

Translating FDA guidance into practice is an ongoing challenge for medical device manufacturers. While the guidance outlines overall goals, it isn't technical, it relies heavily on implementation, and it provides little direction for how to implement objectives. In an ideal world, there would be a checklist of tests, processes, policies, and procedures to follow. In reality, the technology and variables are too complex to make such a checklist possible.

Organizational challenges

Some of the biggest obstacles that medical device manufacturers face when preparing for a PMN or PMA are internal, especially for organizations that have not been through the process.

Organizational and cultural obstacles can include:

- Lack of security in DevOps processes
- Slow, reactive security practices
- Inadequate attention to security
- Lack of accountability for security
- Skills and knowledge gap
- Insufficient budget
- Time constraints
- Inefficient security testing practices

Addressing issues in these areas will not only help manufacturers in their PMN 501(k) and/or PMA process but also shore up their security posture.

Regulatory challenges

According to the Ponemon Institute, only 51% of medical device manufacturers follow FDA guidance to mitigate or reduce security risks in their software.[21] This number reflects the difficulty organizations have in navigating a regulatory environment that is constantly changing and evolving. Product and technology advances outpace the FDA or any regulatory agency's ability to create regulations, so they are continually trying to catch up. Further, the aggregate of regulations in cyber security and healthcare takes a significant toll on an organization's legal, IT, and other resources. Manufacturers must incorporate numerous regulations, many of which are vague and/or redundant. When organizations do achieve compliance, it's never a one-and-done scenario. They must continually invest to keep pace, creating an oddly parallel state: the FDA and other regulators are playing catchup with technology advances while organizations are playing catchup with the regulators.

Best practices for FDA cyber security risk guidelines

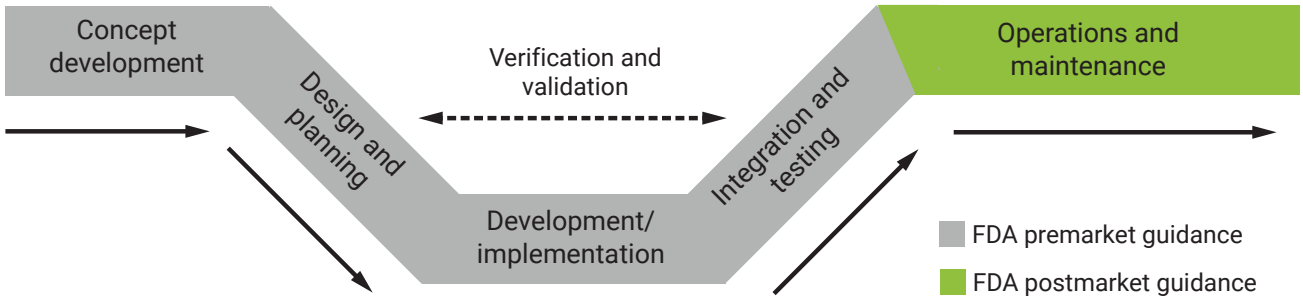
The concept of "reasonable security" is one of the foundations of the FDA. Medical device manufacturers achieve reasonable security only when they treat security as an equal stakeholder in the development process, alongside quality, speed, and other business priorities.

One of the tradeoffs that organizations must constantly balance is the cost of missed deadlines and revenue on the one hand against the cost of insecure software and potential breaches on the other hand.

The best solution is to incorporate security into every phase of development, using risk management processes. In this fashion, security can help organizations achieve the most cost-effective outcomes.

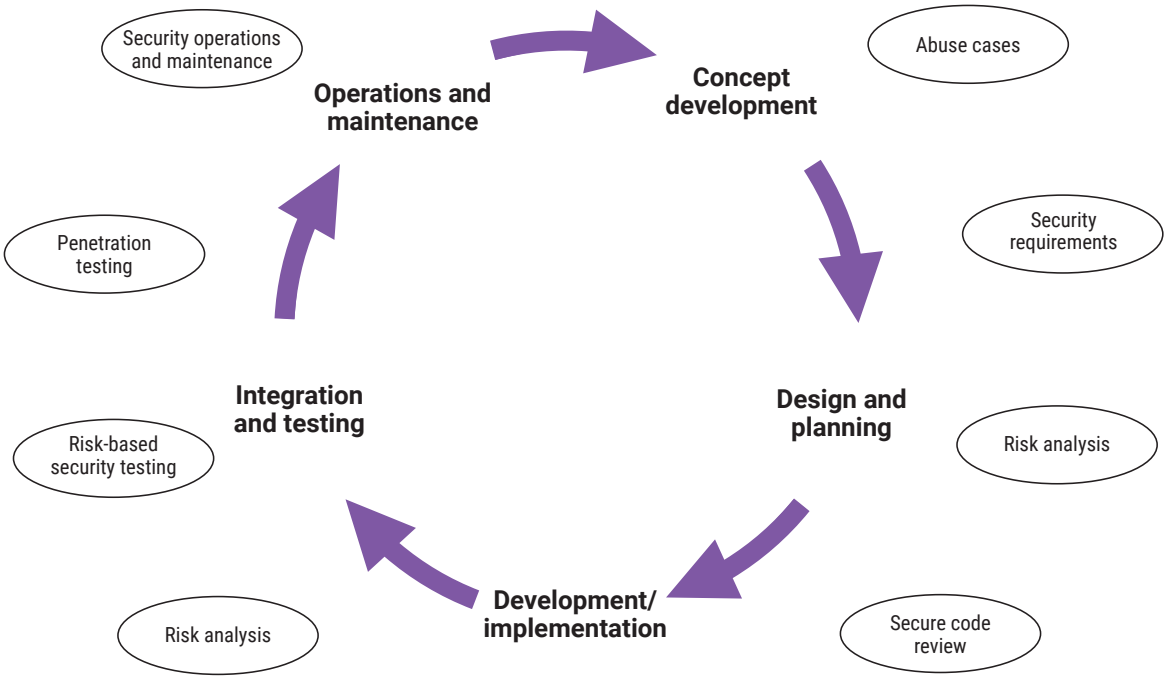
Secure systems or software development life cycle

Medical devices require continuous security and quality maintenance throughout their life cycle, from inception to retirement. With the proper tools and clear staging gates at each phase of the systems or software development life cycle (SDLC), device manufacturers can establish secure practices that address quality, security, and safety to comply with FDA guidance.



Systems development life cycle (systems engineering V model)

FDA premarket and postmarket guidance recommends monitoring, identifying, and addressing cyber security vulnerabilities and exploits as part of the SDLC. Manufacturers should implement integrated security activities such as testing, analysis, verification, attestation, and validation at checkpoints triggered by specific events. The checkpoints should form a governance structure that provides effective risk management while ensuring attainment of business goals.



Software security gates and touchpoints for a secure SDLC

What to secure

The FDA expects medical device manufacturers to perform a risk assessment that addresses all aspects of the IoT. Some systems are straightforward with all parts from the same medical device manufacturer, while others are more complex, with multiple parts and connections. FDA regulatory guidance may be different for each part. FDA premarket review considers how each part contributes to the risk of the overall system. Thus, manufacturers may need additional system-level documentation to demonstrate how all the parts of their devices are reasonably safe and effective.

A typical connected medical device architecture or configuration might include:

- Embedded systems—purpose-built components such as:
  - On-chip memory
  - Microprocessors or controllers
  - Firmware
  - Communication interfaces such as Bluetooth, near-field communications, and other wired protocols, as well as data ports such as universal serial buses, secure digital cards, or multimedia cards
  - Peripheral hardware for auxiliary devices such as data input/output, sensors, and actuators
- Clinician systems
- Mobile devices and applications
- Gateways or hubs
- Cloud services
- Back-end infrastructure
- Websites and APIs
- Third-party integrations

How and when to secure

Security isn't a state or outcome. It's a continuous activity that has integrated touchpoints within the SDLC.

Key activities by SDLC phase

Activity	Concept development	Design and planning	Development/ implementation	Integration and testing	Operations and maintenance
Process analysis and development	•	•			
Threat modeling	•	•			
Architecture risk analysis	•	•	•	•	•
Static analysis			•		
Composition analysis			•		•
Dynamic analysis			•		
Penetration testing				•	•
Cloud and container security assessments				•	•
Mobile application security testing				•	•
Network security testing				•	•

Abuse cases

The security landscape changes quickly. It's important for manufacturers to stay current on attacker threats and techniques so that tomorrow's therapies aren't subject to yesterday's vulnerabilities. Abuse cases allow development teams to think like an attacker to integrate security into concept development, design, and planning. By looking for ways an attacker could bypass existing or missing security controls, they can create new security requirements or acceptance criteria.

Security requirements

Development teams should define high-level security requirements along with functional and nonfunctional requirements, such as requirements to meet various regulatory or reference guidance standards like the FDA guidance and secure coding standards. Ideally these requirements are defined throughout a risk assessment, but it's primarily done in the design and planning phases.

The requirements are identified using a checklist based on predefined elements, but it also involves defining solution-specific requirements through active collaboration between development and security staff. Program and risk assessments help drive security requirements.

Medical device manufacturers can address specific AppSec challenges and objectives by providing an actionable roadmap for security and development teams. This process should include a comprehensive plan to achieve program goals, identify the necessary resources to successfully execute the plan, and implement milestones and metrics to measure success.

Risk analysis

Beginning in the first stages of concept and development, medical device manufacturers must incorporate security into the design. They must employ design analysis techniques like threat modeling and architecture risk analysis to search for security weaknesses in the system architecture. If they aren't specifically looking for security problems in the design, they will miss these security-specific failure modes. Understanding security failure modes is as crucial as, for example, considering biocompatibility failure modes for implantable devices. It requires specific expertise to perform appropriately.

The product development team, including the business owner, should determine a project's intrinsic development risk by completing a risk classification process, which also helps identify the appropriate security activities to perform in subsequent SDLC phases. When an organization is at an advanced maturity level, the security architect also reviews the technical design as a threat modeling or architecture risk analysis exercise. Risk analysis is performed again after the coding phase to confirm that all appropriate security activities were performed.

Risk analysis is primarily influenced by factors that can affect a system's operational context. For example, whether a given function or system element processes personal health information subject to regulatory controls is a factor in determining risk. Additional risks to consider include supply chain, patient safety, and business-related risks.

Threat models

Threat modeling adopts the perspective of malicious actors to see how much damage they can do. It looks beyond canned and well-known threats to examine how the external components medical device manufacturers rely on to build and run their applications can be susceptible to secure design violations, control misconfigurations, security control omissions, or misuse.

A threat model describes a system's attack surface by identifying major software components, assets, threat agents, security controls, and corresponding relationships between objects. It produces a traceability matrix to incorporate into design inputs and regulatory submissions.

Threat models should include:

- Assets prioritized by risk
- Threats prioritized by likelihood
- Attacks that are most likely to occur
- Current countermeasures likely to succeed or fail
- Remediation measures to reduce the threats

Product teams should start thinking about security on day one. Even if a new product is in the ideation stage and just a couple of boxes on a whiteboard, there is enough information to start threat modeling what could go wrong. If the system uses the internet, that's a concern; likewise, a mobile application, patient phone, or wireless communications. Manufacturers can use the information they have to build out specific security actions that can have a big, positive impact on the security of the system.

According to the FDA, "Threat modeling provides a blueprint to strengthen security through the TPLC [total product life cycle] of the devices, thereby ensuring improved safety and effectiveness of medical products. Threat modeling helps lay the groundwork for science-driven penetration testing and other downstream security testing as identified in the 2018 draft premarket guidance."[22]

Architecture risk analysis

Half the software defects that create security problems are design flaws. Therefore, simply testing software for security bugs within lines of code, or penetration testing applications, ignores half the problems that leave systems vulnerable to attack.

Architecture risk analysis is a deeper examination than a threat model that highlights design flaws that automated tools cannot find. It also provides specific mitigation and remediation advice for individual defects. FDA draft guidance requires that manufacturers consider cyber security risks as part of the development process. Architecture risk analysis is a step beyond what is required for cyber security risk management.

Architecture risk analysis enables medical device manufacturers to inspect risk from the inside-out and discover deep-seated design flaws. These assessments use known attack tactics and include a deep dependency analysis. Manufacturers can discover the relationships between major components, assets, and threat agents to find system flaws in an application's design.

Top 10 Security Activities

- **Create a product security working group**
- **Develop system-level security requirements**
- **Offer compliance and security training**
- **Enhances ongoing product support capabilities**
- **Complete design-level risk assessment activities**
- **Establish security documentation**
- **Adopt appropriate automated system analysis tools**
- **Understand open source and vendor risk**
- **Formalize vendor management**
- **Formalize system engineering roles**

Secure code review

As design turns to implementation and testing, the FDA officially recognizes the need for security-focused analysis and testing techniques, including static analysis for proprietary code, composition analysis for open source code, fuzz testing for running applications, and penetration testing. Both the 2018 draft FDA premarket guidance and AAMI TIR57 discuss the need for static and dynamic code analysis, penetration testing, and other technology to manage medical device security risk.

Static analysis

Static code analysis or static application security testing (SAST) systematically scans and applies in-depth tests to identify and eliminate common to critical software security weaknesses in source code. Originally developed to address functional failures, SAST has evolved to become an effective method for enumerating security flaws, particularly the software weakness types known as common weakness enumerators (CWEs).

Composition analysis

Third-party software components don't always provide access to source code, which is necessary for SAST. According to the 2024 "Open Source Security and Risk Analysis" (OSSRA) report, 88% of the audited codebases in the healthcare, health tech, and life sciences industries contain open source code.[23]

Software composition analysis (SCA) helps teams manage the security, quality, and license compliance risks that come with the use of open source and third-party code in applications and containers. Combining SAST and SCA allows medical device manufactures to track and manage security, quality, and license risks and meet FDA premarket guidance.

The NIST, Healthcare Industry Cybersecurity Task Force, and FDA recommend software Bills of Materials (SBOMs) that describe a device's components and any known risks associated with those components, to enable healthcare delivery organizations to determine quickly if they are impacted. A good SCA tool or service should provide an accurate SBOM for any application or container.

An SBOM enables better management of hardware-centric, third-party cyber security risks. FDA 2018 premarket draft guidance emphasizes that SBOMs should include traditional software (including firmware), programmable logic, and hardware. It also outlines how organizations should enumerate commercial, open source, and off-the-shelf software and hardware components that are or could become susceptible to vulnerabilities. The guidance proposes certain key elements of an SBOM for medical devices in support of consistency and standardization.[24]

While SCA is a critical testing method, only 6% of healthcare organizations surveyed in the 2020 "Building Security In Maturity Model" (BSIMM) report had a program for managing open source vulnerabilities.[25]

Dynamic analysis

Dynamic application security testing (DAST) finds real-world risk by simulating attacks and identifying security vulnerabilities while web applications are running, without the need for access to source code.

DAST can use automated tools to identify common vulnerabilities, such as SQL injection, cross-site scripting, security misconfigurations, and others detailed in lists such as Open Web Application Security Project (OWASP) Top 10 web application security risks, CWE top 25 most dangerous software weaknesses, and others.

DAST can also include manual tests to find vulnerabilities that out-of-the-box tools cannot find, such as vulnerabilities related to authentication and session management, access control, information leakage, and more. A manual review can also identify false positives.

Fuzz testing

Fuzz testing can be highly effective in discovering unknown (zero-day) vulnerabilities. A fuzz tester interacts with a running system via its external interfaces, providing malformed data to trigger bad behavior. The scale of this type of testing is broad—from custom, risk-based fuzzing driven from an architecture or source code review to automated fuzzing that generates inputs and runs for hours, days, or weeks, depending on the need.

Medical devices use a diverse set of protocols such as Bluetooth, HL7, and DICOM that have the potential to carry zero-day vulnerabilities. Protocol fuzzing can proactively detect security defects during development and testing, so manufacturers avoid having to respond to breaches and device failures in the field.

Penetration testing

Penetration (pen) testing can extend DAST by using multiple testing tools and in-depth manual tests to find vulnerabilities in business logic and try to exploit them. It is a point-in-time assessment against current, known security risks and involves security verification and validation, which is the final layer of testing designed to simulate real-world attacks on a target system.

Pen testing for embedded software-only systems helps manufacturers identify and resolve risks—and prevent them from reoccurring. Manufactures can perform or hire a team to perform high-quality, multidepth pen testing for embedded devices, mobile apps, and applications at any stage of the SDLC.

The primary goal of pen testing is to identify potential security vulnerabilities in a real-world implementation environment. Manufacturers typically conduct these tests from the standpoint of an attacker, focusing on the exposure of the system to threats from various entry points. Manual testing can reveal business logic flaws as well.

Risk-based security testing

After development, manufacturers should perform security testing during the quality assurance phase to validate the security requirements. Manual and automated testing activities, as well as their evaluation criteria, are based on the risk profile of the system being tested.

Areas to conduct risk-based security testing include the cloud and containers, mobile applications, and the network.

Cloud and container security assessments

Medical device manufacturers should appraise how they implement cloud security controls in their environments and evaluate the architecture of the security controls in their cloud applications. A cloud architectural risk analysis shows where security controls are insufficient and outlines how to improve them. A cloud configuration review reveals whether a cloud configuration stands up to security checks.

Mobile application security testing

Mobile application security testing (MAST) combines static and dynamic testing techniques to discover vulnerabilities in iOS and Android apps and their back-end components. MAST enables medical device manufacturers to implement client-side code, server-side code, and third-party library analysis quickly, so they can find and fix security vulnerabilities systematically in their mobile applications, without needing to access source code.

Network security testing

Network security testing (NST) detects common to critical vulnerabilities in external networks and systems through automated scanning with manual triage. NST checklists may include test cases for encrypted transport protocols, SSL certificate scoping issues, use of administrative services, and more.

Security operations and maintenance

Security operations generally entail the protection and monitoring of the system after initial deployment and throughout its life cycle. Operations and maintenance activities around changes, upgrades, retirement, and replacement of devices and their applications include gathering feedback from customers and the field, monitoring alerts and warnings about new vulnerabilities and regulation updates, implementing patches and remediation, and communicating cyber security incidents and end-of-life information to regulatory authorities and customers.

Supporting activities

Medical device manufacturers need both organizational and security-focused activities to support a security touchpoints implementation.

Security training

Security training is one of the most important activities a medical device manufacturer can undertake to facilitate a robust systems security program. Training contributes to improved interpretation of test findings, more-informed decision-making, and a culture of security throughout the organization.

Training topics include threat modeling, architecture analysis, software security fundamentals, security requirements, defensive programming, secure code review, and more. It should be tailored to individual roles and responsibilities.

Security libraries

Medical device manufacturers can reduce implementation variance and errors, and increase productivity by maintaining security libraries and design patterns. Security libraries enable developers and engineers to find vetted solutions and implementation help with common security functions.

Open source risk intelligence

Many systems use open source libraries to support application or system functions. Understanding the risk that these libraries may introduce into a system is critical to addressing overall risk. Developers should identify and evaluate open source components and monitor their security status. Open source risk intelligence is a process that supports the output of SCA.

Attack intelligence and sharing

Maintaining awareness of current attack patterns and vulnerabilities can facilitate risk analysis activities. This intelligence—which includes activities such as threat intel monitoring, security topic awareness, training, conferences, and knowledge building and sharing—helps medical device manufacturers understand the potential attack landscape that drives security requirements and implementation characteristics.

Manufacturers should participate in information-sharing organizations such as Health-ISAC that enable members to take vulnerability data to their own teams and assess their devices' exposure to these issues. They should also develop a coordinated vulnerability disclosure policy to manage activities across the organization and with customers.

Policy and documentation

To develop a complete security program, medical device manufacturers should analyze their internal culture and documentation hierarchy to identify what artifacts and programs would assist them in achieving their objectives. Many security efforts fall out of use when not bolstered by internal processes that business owners and compliance personnel maintain. Cyber security documentation should include design documentation, system diagrams, a system threat model, and risk management documentation.

Conclusion

Achieving the FDA baseline of reasonable security in medical devices requires continuous support in navigating the security and regulatory landscape. It also requires a security program that is informed and enforced by a secure SDLC and that enables the business through appropriate risk management and tradeoff decisions.

Navigating the medical device security landscape can be complex, so it's especially important that manufacturers select a vendor with medical device security knowledge and expertise.

Black Duck is the recognized leader in software security. We are actively involved in medical and healthcare industry efforts to help clients build more-secure care-delivery systems. We are a key contributor to the secure design guidance documentation put out by leading agencies, consortia, and working groups. Our team collaboratively creates secure design guidance documents through the AAMI working groups, including "Avoiding the Top 10 Software Security Design Flaws" and "Building Code for Medical Device Software Security by the Institute of Electrical and Electronics Engineers (IEEE)." We have also worked with the Archimedes Group at the University of Michigan, IEEE, National Science Foundation, Health-ISAC, and the FDA to help healthcare companies combat cyber criminals.

Black Duck customers include the top 10 medical device manufacturers and 4 of the top 5 managed healthcare firms.

In addition, the Black Duck services team has assessment experience with a broad range of medical and nonmedical embedded systems, including implanted medical devices, drug delivery systems, surgical imaging systems, ATMs, gaming consoles, and smart meters. When working with Black Duck, manufacturers benefit from the innovations of multiple industries.

Learn how Black Duck can help you build secure medical devices that comply with FDA guidance.

Endnotes

1 David R. Ramsdale, Archana Rao, Cardiac Pacing and Device Therapy, Springer, 2012

2 Oleg Bestsennyy, Greg Gilbert, Alex Harris, Jennifer Rost, Telehealth: A quarter-trillion-dollar post-COVID-19 reality? McKinsey & Company, July 9, 2021.

3 U.S. Food and Drug Administration, 510(k) Clearances, June 9, 2021.

4 Protenus and DataBreaches.net, 2021 Breach Barometer, Protenus, Inc., 2021.

5 Sara Mitran, Medical Device and Network Security: Coming to terms with the Internet of Medical Things, Frost & Sullivan, 2019.

6 Ponemon Institute, Medical Device Security: An Industry Under Attack and Unprepared to Defend, Black Duck, 2017.

7 Chris Sherman, Salvatore Schiano, Best Practices: Medical Device Security. Forrester Research, 2019.

8 Paul Sisson, Scripps ransomware shutdown hits the two-week mark, The San Diego Union-Tribune, May 14, 2021.

9 Nicole Perlroth, Adam Satariano, Irish Hospitals Are Latest to Be Hit by Ransomware Attacks, The New York Times, May 20, 2021.

10 Federal Bureau of Investigation, Cyber Division, FBI TLP White Flash Alert: Conti Ransomware Attacks Impact Healthcare and First Responder Networks. American Hospital Association, May 20, 2021.

11 Ariel Hart, Cyber attack disrupts cancer care, The Atlanta Journal-Constitution, April 27, 2021.

12 Ponemon Institute, Medical Device Security: An Industry Under Attack and Unprepared to Defend, Black Duck, 2017.

13 Sedgwick, 2021 Recall Index Report, United States Edition, 2021.

14 Christina Jewett, Hidden FDA Reports Detail Harm Caused By Scores of Medical Devices, KHN.org, March 7, 2019.

15 U.S. Food and Drug Administration, Classify Your Medical Device, 2020.

16 Ibid.

17 Ibid.

18 U.S. Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices, December 28, 2016.

19 Ibid.

20 Ibid.

21 Ponemon Institute, Medical Device Security: An Industry Under Attack and Unprepared to Defend, Black Duck, 2017.

22 U.S. Food and Drug Administration, FDA CDRH and Medical Device Security: Response to NIST Regarding President's Executive Order (EO) on Improving the Cybersecurity of the Federal Government (EO 14028), 2021.

23 Black Duck, Open Source Security and Risk Analysis, 2021.

24 U.S. Food and Drug Administration, FDA CDRH and Medical Device Security: Response to NIST Regarding President's Executive Order (EO) on Improving the Cybersecurity of the Federal Government (EO 14028), 2021.

25 Black Duck, Building Security In Maturity Model, 2021.

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.