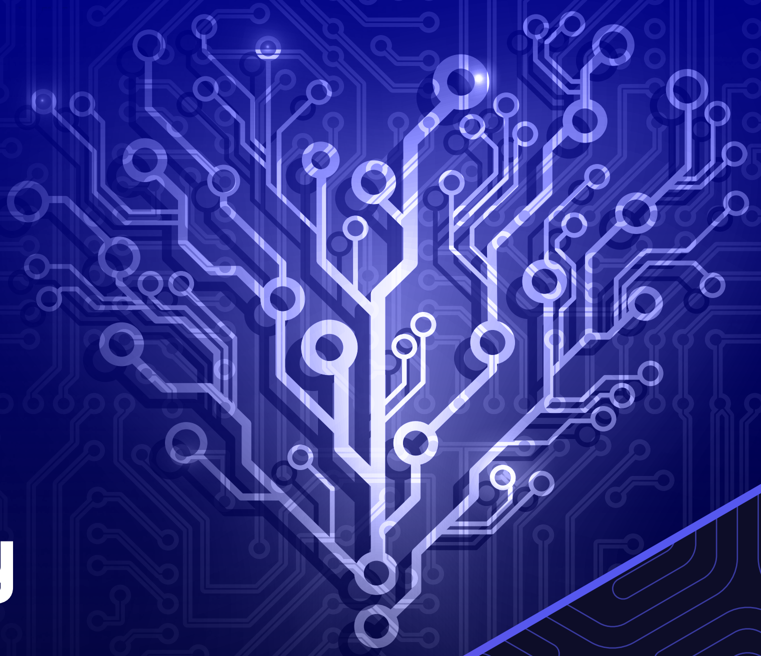
praetorian

WHITE PAPER

FDA Premarket and Postmarket Medical Device Cybersecurity

Robust cybersecurity leads to greater patient impact.



Inside this Report

March 2024

Introduction

Medical devices have significantly evolved since 1976, when the FDA first began regulating them. The advancement in related sciences has shifted the industry from mechanical products to modern cloud-connected devices. For example, before 2009, adjusting a pacemaker required a doctor to perform surgery to access the mechanical device within their patient. Today, wireless-enabled pacemakers allow healthcare providers to monitor their patients' heart rhythms remotely and make necessary adjustments.

The FDA, subject to the complexities of modern government and a rapidly evolving medical technology space, had been slow to adapt their regulations to keep up with the ever-changing medical technology landscape. For instance, wireless pacemakers, faced a recall in 2017 due to concerns that the devices were vulnerable to hacking attacks. This cybersecurity vulnerability profoundly damaged the manufacturer's reputation, revenue, and most importantly, posed a serious threat to human life. Cybersecurity has since become a critical element of ensuring the overall safety of medical devices, making the industry one of the most heavily regulated in the world.

In March 2023 Congress granted the FDA authority to enforce cybersecurity regulations. The strategies organizations adopt for their premarket submissions and post market monitoring will now directly affect the likelihood of their medical devices receiving market release approval from the FDA. While various cybersecurity approaches and implementations exist, selecting a holistic offensive security strategy that covers the full lifecycle will be the most effective way manufacturers can ensure their devices not only make it to market, but remain secure into the future.

Since 2018, medical device manufacturers have been aware of the guidelines in "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices." In this document, the FDA emphasized the importance of cybersecurity risk management throughout the product lifecycle and included suggestions for the following:

- Addressing vulnerabilities
- Implementing design controls
- Establishing a coordinated vulnerability disclosure policy.

However, for the five years that version of the document was in effect, the FDA lacked authority to enforce these guidelines. The document neither provided instructions on how to perform recommended penetration testing nor outline consequences for manufacturers that did not plan for their medical devices' cybersecurity. Medical device manufacturers could determine for themselves whether to develop a cybersecurity risk management plan, and how to incorporate any testing into it.

The key shift occurred in March 2023 when the Consolidated Appropriations Act of 2023 granted the FDA the authority to enforce the guidelines as requirements (see article). The basic steps to ensure compliance remain the same; the difference is that the FDA can now reject medical devices that do not meet their baseline cybersecurity standards. To facilitate successful medical device development and release, the FDA has set clear expectations for manufacturers to demonstrate their commitment to cybersecurity throughout the product lifecycle.

October 2023 FDA Regulatory Changes

A grace period before the FDA began enforcement was granted until October 1, 2023. After this date, the new requirements would be enforced on both new and existing medical devices. The FDA has already begun enforcing these requirements on some manufacturers submitting modifications to existing devices under the 510(k) application process. Even devices initially submitted with a 510(k) exception application may now be subject to the cybersecurity testing requirements.

Importance of a Third-Party Partner

The cybersecurity regulations now emphasize the need for manufacturers to collaborate with third-party security experts to achieve robust security. Medical device manufacturers aiming to bring their products to market must conduct comprehensive risk assessments and implement security controls to mitigate threats. However, internal cybersecurity teams focusing on compliance may lack the attacker perspective necessary to be effective in those tasks. Partnering with a third-party cybersecurity provider in both the premarket submission process and postmarket monitoring can offer manufacturers an offensive security strategy that better meets FDA requirements.

In addition to developing and executing an offensive security strategy for a medical device, external experts can assist the manufacturer's internal teams manage the implications of this strategy. Key areas of potential impact include the following FDA requirements:

Robust premarket testing and comprehensive risk assessments.
A third-party partner with an offensive security focus can provide increased confidence that the cybersecurity strategy considers the full range of potential threats.

Continuous offensive security (COS) postmarket integration.
A partner specializing in COS understands the need for ongoing vigilance to address evolving threats, allowing the team to focus on other priorities.

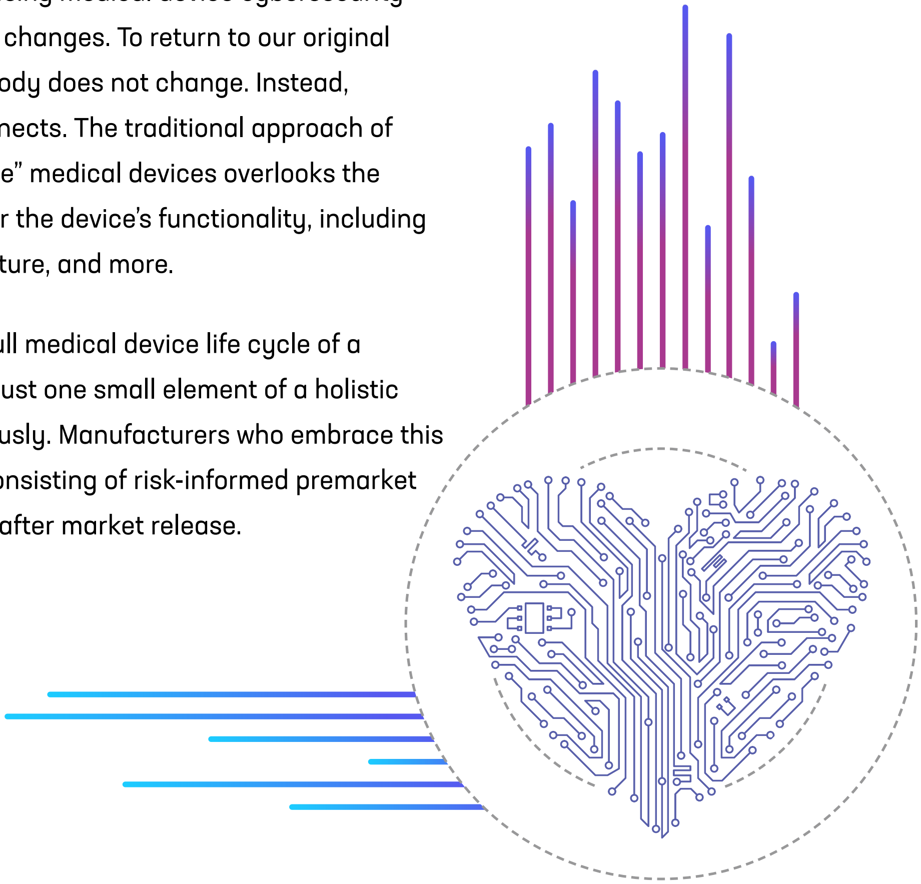
Collaboration with third-parties.
Maintaining a strategic partnership with a single offensive security vendor minimizes the internal team's burden of onboarding new vendors.

Security control implementation.
A third-party partner with an attacker-focused approach can guide internal security teams on effective controls that truly mitigate threats rather than simply fulfilling a requirement.

Offensive Security Strategy for the Full Medical Device Life Cycle

An important distinction to consider when discussing medical device cybersecurity is that the environment is often the element that changes. To return to our original example, a pacemaker implanted in a patient's body does not change. Instead, what changes is the environment to which it connects. The traditional approach of conducting a one-time penetration test to "secure" medical devices overlooks the dynamic nature of everything that is essential for the device's functionality, including the applications, databases, the cloud infrastructure, and more.

Planning an offensive security strategy for the full medical device life cycle of a medical device acknowledges that the device is just one small element of a holistic environment that must be safeguarded continuously. Manufacturers who embrace this approach establish a robust two-part strategy consisting of risk-informed premarket assessments and continuous proactive security after market release.



Premarket Submissions: Cybersecurity in Development

The FDA requires manufacturers to provide various documents depending on the medical device being submitted for market approval. These documents include the 510(k), Premarket Approval (PMA) Application, and De Novo. The review process can take an average of eight months. Incorporating a cybersecurity strategy early into the project allows the device team more time to address and mitigate any vulnerabilities the process uncovers.

The FDA has outlined that medical devices submitted for premarket approval must include, at a minimum:

Cybersecurity Bill of Materials (CBOM)

The FDA emphasizes the importance of maintaining an accurate Software Bill of Materials (SBOM) as it aids in the management of cybersecurity risks throughout the software stack, as mentioned in the “Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions” guidance. An SBOM should include both the manufacturer-developed components and third-party components such as purchased/licensed software, open-source software, and the upstream dependencies required by these components. A vulnerability analysis of the software listed in the bill of materials should also be included, also known as a CBOM.

Security Control Listing and Verification

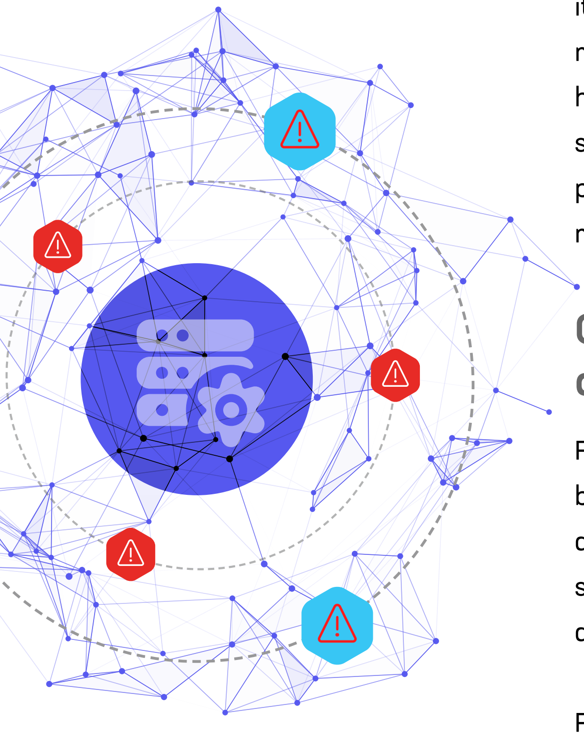
A listing of security controls present on a device should be provided, alongside an analysis of what risks a given control may mitigate. An adequate list of security controls should, at a minimum, include controls that fit into the following categories.

- ✓ Authentication
- ✓ Authorization
- ✓ Cryptography
- ✓ Code, Data, and Execution Integrity
- ✓ Confidentiality
- ✓ Event Detection and Logging
- ✓ Resiliency and Recovery
- ✓ Updatability and Patchability

Another key part of the security control identification process is verification that controls are functioning as they should be. From the ESTAR submission template, the risk management report should include “traceability to the verification reports for documented security controls”. Included in our Premarket Control Verification is a listing of the controls tested by our security team, with each one categorized using this criteria.

Threat Modeling

Threat modeling serves as an essential tool to assess the threats posed to networks, applications, and systems interacting with medical devices. The FDA requires a submission of a comprehensive threat model that goes beyond just the medical device itself. It requires giving due consideration to all potential interactions between the medical device and auxiliary systems like external management systems, web apps, and the broader healthcare IT infrastructure. These peripheral entities can introduce risks to the medical device or may become direct targets for hostile agents. The FDA emphasizes that the threat modeling procedure should cater to threats posed by active adversaries and malicious use, and should adopt a forward-thinking approach to predict and prevent attempts to exploit systems linked to the medical device. Additionally, it's essential that this threat modeling be integrated with conventional risk management strategies and failure mode analysis techniques to enable a holistic risk assessment encompassing all plausible risk domains. As a company specializing in offensive security, we at Praetorian have unparalleled experience performing threat modeling, and listing out all potential threats that systems may face.



Cybersecurity Risk Assessment and Exploitability Analysis

Risk assessment of vulnerabilities, software anomalies, and a harm analysis based on the discovered risk. In the most recent version of the ESTAR template and its related guidance, it is called out that an assessment of exploitability should be used to inform risk management practices, rather than quantitative risk analysis.

From the FDA's perspective, this approach to cybersecurity demonstrates the manufacturer's commitment to risk management. Undertaking a comprehensive risk assessment beginning in the development phase, then documenting follow-on penetration testing and control implementation throughout the cycle, also can help streamline the approval process. Fewer material vulnerabilities in a submission translates to fewer issues requiring resolution before the FDA can grant approval. Therefore, this approach to preparing for the premarket submission process constitutes the first half of an effective offensive security strategy for medical devices.

Postmarket Management: Continuous Offensive Security

The FDA's expanded regulatory authority includes assessing medical device manufacturers' plans for postmarket monitoring, to ensure the ongoing safety and efficacy of the devices it approves. The now-enforceable regulations emphasize the importance of continually monitoring for, identifying, and remediating cybersecurity vulnerabilities as part of postmarket device management. This task is an ideal use case for COS, which involves attack surface management (ASM), continuous red teaming, and managed offensive security.

COS with a third-party partner, therefore, should comprise the second half of any effective offensive security strategy. For further details on COS, specifically, see our white paper on the topic.

Attack Surface Management.

By constantly monitoring the attack surface (various entry points attackers can use to gain access to a medical device) via automated tools, manufacturers can understand their true exposure and effectively prioritize remediation.

Continuous Red Teaming

By simulating real-world attack scenarios on a regular cadence, medical device companies can validate threats to stay ahead of attackers.

Managed Offensive Security

By partnering with an offensive security provider, internal teams can augment their capabilities while reducing their costs.

Praetorian's Approach to Medical Device Cybersecurity

Praetorian's team of product security engineers has extensive experience working with manufacturers developing and bringing medical devices to market. Since 2018, we have followed the FDA's guidelines as enforceable requirements, and we have encouraged our clients to do the same. We have successfully guided over 88 medical devices to market, gaining a deep understanding of the FDA's regulations, processes, and the potential roadblocks device teams might encounter. Furthermore, we stay informed about the latest updates from the FDA, and are always prepared to help clients evaluate and adapt their strategies to account for new developments.

Tailor the Solution

Every medical device is unique, as are its cybersecurity requirements. Therefore, Praetorian customizes the offensive security strategy for each device. Yet the goal remains the same for every partnership: to ensure comprehensive protection and, through that, compliance with the FDA's requirements. Manufacturing partners gain access to our experts in medical device security. Our team's two-part focus is providing clear, actionable feedback to prevent security vulnerabilities during development, and continuously identifying and mitigating emerging threats postmarket.

Our team will provide services that match the following FDA ESTAR template requirements, and will collaborate with manufacturers to ensure the submission meets their rigorous standards.

Cybersecurity Risk Assessment and Exploitability Analysis:

Our risk-informed security assessment of a medical device begins with a careful evaluation of it's purpose, users, and attack surface. Drawing on our decades of offensive security experience and apply it to a manufacturer's product and the systems it interacts with. Included in this service is vulnerability analysis, penetration testing, attack surface analysis, and an exploitability analysis of any discovered security issues. This ensures a manufacturer's Cybersecurity Risk Assessment file is well-informed and complete.

Threat Modeling

Utilizing our Process for Attack Simulation and Threat Analysis (PASTA) methodology, we create a comprehensive threat model based on the system design, previous work performed on the device, input from a manufacturer's stakeholders, and our own analysis. This information directly informs the Security Control Listing requirement, as we will also map out mitigating controls in place.

Security Control Listing and Verification

In addition to the controls discovered during the Threat Modeling and Cybersecurity Risk Assessment, we take input from a manufacturer's stakeholders to identify other controls that are in place on a device. Test cases are developed and executed to verify each control listed, and categorized as defined and required by the FDA.

Cybersecurity Bill of Materials (CBOM)

We review the Software Bill of Materials provided and conduct testing of any off-the-shelf software or dependencies used by the device. This ensures the device and the related systems remain protected from supply or dependency chain attacks.

Cybersecurity Management Plan

Our Advisory Services team collaborates with clients to ensure that the management plan accounts for both current and emerging threats, safeguarding the device throughout its entire lifecycle. Ensuring that the Cybersecurity Management Plan is accurate and that systems are in place to support it is critical to ensuring postmarket cybersecurity requirements are met.

As your trusted partner, we are always happy to answer questions, offer guidance, and assist with requirements beyond those mentioned above.

Reduce Cybersecurity Costs

Our offensive security strategy for securing medical devices has a proven track record of identifying and remediating vulnerabilities across the entire life cycle, which has helped manufacturers accelerate the FDA approval process. Our partners have been able to outsource cybersecurity tasks to our team, allowing them to focus on their own core competencies. By shortening the time to market and enabling internal teams to redirect their efforts, manufacturers who have partnered with us have minimized expenses associated with managing the cybersecurity risk for their devices.

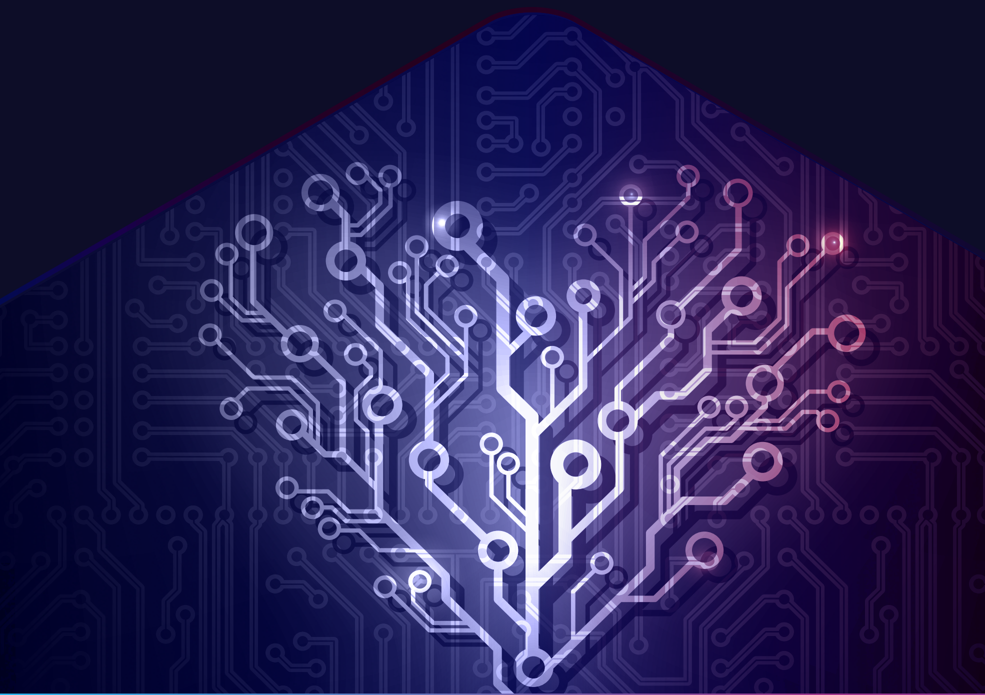
Increase Market Share

Protecting patients' safety and data is vital to maintaining brand reputation and increasing customer loyalty. A robust cybersecurity posture, such as the one medical device manufacturers can establish with an offensive security strategy, results in more secure devices. When healthcare providers and their patients feel confident that a manufacturer has taken the FDA's requirements seriously, and will continue to do so, their medical devices ultimately gain larger market share.

Offensive Security Strategy Yields Compliance

March 2023's expansion of the FDA's ability to enforce cybersecurity requirements for medical devices means manufacturers must develop a strategy to comply with these regulations as they develop and release new products. Due to insufficient resources within internal teams, partnering with a third-party can be a force multiplier in the premarket submission and postmarket monitoring process. However, to maximize the value a third-party can add, manufacturers should choose a partner with an expertise in offensive security, capable of tailoring a full lifecycle strategy for each unique medical device entering the market. Adopting this strategy will ultimately result in quicker market entry for manufacturers, as they satisfy the FDA's requirements more efficiently.

More importantly, applying an offensive security strategy to medical device cybersecurity is about embracing the holistic nature of the technology and the industry. Simply meeting regulatory requirements is not enough to ensure genuine security, as doing the bare minimum will merely fulfill the FDA's criteria. Manufacturers who prioritize the development of a strong cybersecurity strategy will produce more secure devices and have a more profound impact on patients' lives while inherently satisfying the FDA's requirements.



twitter.com/praetorianlabs

facebook.com/praetorianlabs

linkedin.com/company/praetorian

youtube.com/user/PraetorianLabs

github.com/praetorian-inc