PRAETORIAN

WHITE PAPER

FDA Premarket and Postmarket Medical Device Cybersecurity

Robust cybersecurity leads to greater patient impact.

INSIDE THIS REPORT

INTRODUCTION

The Evolution of Medical Device Security

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.

REGULATORY CHANGES

March 2023: FDA Gains Enforcement Authority

In March 2023, Congress granted the FDA authority to enforce cybersecurity regulations. The strategies organizations adopt for their premarket submissions and postmarket 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.

Historical Context

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:

- **Addressing vulnerabilities** - Proactive identification and mitigation of security flaws
- **Implementing design controls** - Security built into the development process
- **Coordinated vulnerability disclosure** - Processes for reporting and addressing security issues

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 outlined consequences for manufacturers that did not plan for their medical devices' cybersecurity.

REGULATORY CHANGES

October 2023 FDA Regulatory Changes

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. 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.

> **Enforcement Date:** 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.

PARTNERSHIP

Benefits of a Third-Party Security Partner

Internal cybersecurity teams focusing on compliance may lack the attacker perspective necessary to be effective. 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.

Robust Testing
Comprehensive risk assessments and premarket testing

Continuous COS
Ongoing offensive security integration postmarket

Collaboration
Strategic partnership minimizes vendor onboarding burden

Security Controls
Attacker-focused approach guides effective control implementation

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.

> **A third-party partner with an offensive security focus can provide increased confidence that the cybersecurity strategy considers the full range of potential threats.**

STRATEGY

Offensive Security Strategy for the Full Medical Device Lifecycle

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 lifecycle 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:

1. **Risk-Informed Premarket Assessments**
   Comprehensive security evaluation during development to identify and mitigate vulnerabilities before market release
2. **Continuous Proactive Security Postmarket**
   Ongoing monitoring, testing, and threat response to maintain security throughout the device's operational life

PREMARKET

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.

Required Documentation

- **Cybersecurity Bill of Materials (CBOM)** - Software components and vulnerability analysis
- **Security Control Listing and Verification** - Authentication, authorization, cryptography, integrity, logging, resiliency, and patchability controls
- **Threat Modeling** - Comprehensive assessment of threats to the device and connected systems
- **Cybersecurity Risk Assessment and Exploitability Analysis** - Risk-based evaluation of discovered vulnerabilities

> **Fewer material vulnerabilities in a submission translates to fewer issues requiring resolution before the FDA can grant approval.**

POSTMARKET

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.

Attack Surface Management
Constant monitoring of entry points attackers can use to gain access to medical devices

Continuous Red Teaming
Simulating real-world attack scenarios to validate threats and stay ahead of attackers

Managed Offensive Security
Partnering with security experts to augment internal capabilities while reducing costs

OUR APPROACH

Praetorian's Approach to Medical Device Cybersecurity

88+

MEDICAL DEVICES SUCCESSFULLY GUIDED
TO MARKET BY PRAETORIAN

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.

Tailored Solutions

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.

> **Our team's two-part focus:** Providing clear, actionable feedback to prevent security vulnerabilities during development, and continuously identifying and mitigating emerging threats postmarket.

SERVICES

Our FDA-Aligned Services

- **Cybersecurity Risk Assessment and Exploitability Analysis** - Risk-informed security assessment with vulnerability analysis, penetration testing, and attack surface analysis
- **Threat Modeling** - PASTA methodology creating comprehensive threat models based on system design and stakeholder input
- **Security Control Listing and Verification** - Test case development and execution to verify each control as required by the FDA
- **Cybersecurity Bill of Materials (CBOM)** - Review and testing of off-the-shelf software and dependencies
- **Cybersecurity Management Plan** - Collaboration to ensure the plan accounts for current and emerging threats

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.

Increase Market Share

Protecting patients' safety and data is vital to maintaining brand reputation and increasing customer loyalty. A robust cybersecurity posture results in more secure devices and ultimately gains larger market share.

CONCLUSION

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 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.**

Ready to Secure Your Medical Devices?

Partner with Praetorian to navigate FDA requirements and protect patient safety.

Contact Us