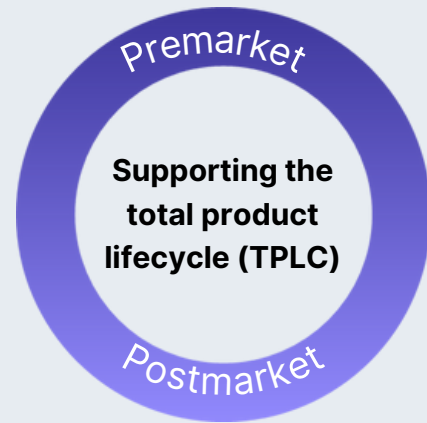# Medcrypt

Medcrypt Services:
Cybersecurity Regulatory Compliance for Medical Devices

Medcrypt's cybersecurity services - led by former FDA policy experts - streamline compliance, enhance security, and protect your devices from development to postmarket.

Premarket

Supporting the total product lifecycle (TPLC)

Postmarket

The Medcrypt difference

- **Reduce** AINN response time from **180 days to just 45-60 days, with a 100% approval rate**
- Since 2023, **100%** of customers using Medcrypt services have **successfully achieved FDA approval**
- **200+ projects** have been successfully completed across **60+ clients**

Premarket Services

Regulatory Cybersecurity Readiness
Navigate regulatory complexities with ease. Whether preparing a submission or addressing FDA requests for additional information, our experts work with you to achieve FDA clearance or approval efficiently.

FDA Hold Letter Response
In the event of an FDA hold letter, Medcrypt provides immediate guidance to navigate the response process effectively.

Threat Modeling & Risk Mitigation
Navigating FDA cybersecurity requirements is complex. Our experts simplify the process using the TIR-57/SW96 framework, helping you develop or refine your Threat Model and Cybersecurity Risk Assessment to align with your device's Risk Management Process from analysis to review.

PKI & Cryptography Analysis
Ensure a secure foundation with expert analysis of and improvement for your cryptographic design, including assessments that any PKI employed follows best practices and aligns with regulatory expectations to strengthen device security at scale

Cybersecurity Maturity Assessments
Advance your security posture with a tailored assessment that benchmarks your security capabilities, identifies gaps, and provides a roadmap for improvement.

Secure Development Lifecycle (SDLC) Integration
Our experts help you integrate SBOM validation and software update mechanisms into your development process, ensuring compliance with FDA expectations and enhancing cybersecurity resilience.

Medical device cybersecurity doesn't stop at FDA approval. Postmarket compliance ensures ongoing patient safety, regulatory adherence, and device integrity in an evolving threat landscape. Medcrypt's services help manufacturers maintain regulatory cybersecurity compliance and safeguard device integrity against emerging threats after FDA approval.

Postmarket Services

Cybersecurity Incident Response
Prepare for real-world threats with our Incident Response Tabletop Exercise. We simulate attacks to test, refine, and validate your response plans - ensuring proper preparation; rapid detection; effective containment and appropriate follow-up; reducing impact and protecting your company's reputation.

Vulnerability Management & Patch Strategy Development
We'll work with you to establish robust processes for continuous monitoring of vulnerabilities and threats. This includes developing regulatory-compliant patching and update strategies to ensure the ongoing integrity of your medical devices and generate metrics to track your successes.

Cybersecurity Risk Management
Assess your security posture, prioritize risks, and develop a strategic roadmap for continuous improvement. We align security investments with industry standards to drive best-in-class protection.

SBOM Validation & Monitoring
Automated SBOM validation and monitoring to track and mitigate emerging vulnerabilities in third-party components.

Regulatory Change Management & Compliance Updates
Proactive tracking of evolving cybersecurity regulations, including FDA and global requirements, with strategic guidance to keep your device security and documentation aligned with the latest compliance expectations.

Ensure your medical device is secure by design and regulatory-ready.
Contact our team for a cybersecurity consultation today at info@medcrypt.com