Scribe

Scribe Use Case:

Empowering Cybersecurity Compliance for Medical Devices

How Scribe Security Helps Medical Device Manufacturers Meet FDA Cybersecurity Guidelines

Additional information is available at https://scribesecurity.com/

Scribe

Empowering Cybersecurity Compliance for Medical Devices

How Scribe Security Helps Medical Device Manufacturers Meet FDA Cybersecurity Guidelines

---

Executive Summary

As medical devices become increasingly connected and software-driven, ensuring robust cybersecurity is critical for patient safety and regulatory compliance. The FDA's Cybersecurity in Medical Devices Guidelines outline stringent requirements for risk management, secure software development, and ongoing vigilance throughout a device's lifecycle. Scribe Security's comprehensive software supply chain security platform generates SBOM and manages the associated risk from throughout the SDLC, embeds security directly into the software development lifecycle (SDLC), automates continuous attestations, and generates verifiable evidence—providing medical device manufacturers with the tools they need to meet FDA requirements and safeguard their products.

Introduction

The rapid evolution of medical device technology has transformed healthcare, but it also introduces new cybersecurity risks. Recognizing these challenges, the FDA has issued guidelines that demand a proactive, evidence-based approach to cybersecurity throughout the SDLC and across the software supply chain. Manufacturers must ensure that every software component—from development to deployment— has an SBOM and is secure by design.

Scribe Security's platform addresses these challenges head-on. By integrating seamlessly into DevOps toolchains and automating security attestations, our solution enables manufacturers to collect required security evidence and maintain rigorous cybersecurity standards while streamlining compliance and reducing manual overhead.

FDA Cybersecurity Guidelines for Medical Devices

The FDA's guidelines for cybersecurity in medical devices emphasize several core areas:

- **Risk Management and Threat Modeling:** Manufacturers must conduct thorough risk assessments and continuously monitor emerging threats.
- **Secure Software Development:** Security must be embedded into every phase of the SDLC, with documented processes for identifying and mitigating vulnerabilities.
- **Software Supply Chain Security:** Comprehensive visibility into all software components (including third-party code) is required, often through Software Bills of Materials (SBOMs).
- **Post-Market Surveillance and Incident Response:** Manufacturers need robust processes for monitoring, reporting, and remediating vulnerabilities throughout a device's lifecycle.
- **Documentation and Evidence:** Clear, auditable evidence of security controls and compliance must be maintained for regulatory review.

Challenges Facing Medical Device Manufacturers

Medical device manufacturers face unique cybersecurity challenges:

- **Complex Software Ecosystems:** Devices often incorporate diverse software components, increasing the potential for vulnerabilities.
- **Manual Compliance Processes:** Traditional approaches to compliance are labor-intensive and prone to error, making it difficult to provide consistent, auditable evidence.
- **Rapid Development Cycles:** The pressure to innovate quickly can compromise the thoroughness of security reviews.
- **Evolving Threat Landscape:** Cyber threats evolve rapidly, necessitating continuous monitoring and agile risk management.

How Scribe Security Addresses FDA Cybersecurity Requirements

Scribe Security's platform is purpose-built to help medical device manufacturers navigate and comply with FDA cybersecurity guidelines. Here's how:

1. Automated Security Attestations Across the SDLC

- **Continuous Evidence Generation:**
  Scribe integrates directly into CI/CD pipelines, automatically capturing and cryptographically signing security evidence at every stage of development. Each code commit, build artifact, and dependency update generates a machine-readable attestation that provides undeniable proof of compliance.

- **Machine-Readable Documentation:**
  The platform converts security data into standardized, machine-readable formats, enabling automated audits and seamless submission of evidence during FDA inspections.

2. Comprehensive Software Supply Chain Visibility

- **Multi-Stage SBOM Generation:**
  Scribe automatically produces detailed Software Bills of Materials (SBOMs) that document all components and dependencies used in a device's software. This transparency is crucial for identifying vulnerabilities in third-party code and ensuring that every element meets security standards.

- **End-to-End Provenance Tracking:**
  By tracking the origin and integrity of every software component through continuous code signing and in-toto attestations, Scribe offers a robust chain-of-custody that supports rapid incident response and remediation.

3. Embedded Security Controls (Guardrails-as-Code)

- **Automated Compliance Enforcement:**
  Scribe embeds security guardrails into DevOps workflows, ensuring that only software meeting predefined security criteria progresses through the pipeline. If a code change fails to meet these mandatory requirements, it is automatically halted—preventing non-compliant software from entering production.

- **Real-Time Risk Mitigation:**
  Continuous monitoring and automated alerts enable manufacturers to detect and

remediate vulnerabilities promptly, reducing the risk of cyber incidents.

4. Evidence-Based Reporting for Regulatory Audits

- **Automated Compliance Reporting:**
  The platform generates comprehensive, evidence-based reports that document adherence to FDA cybersecurity guidelines. These reports include detailed logs of security attestations, SBOMs, and remediation actions.

- **Audit-Ready Documentation:**
  With Scribe, manufacturers can provide regulators with a complete, immutable record of their security controls—simplifying the audit process and building trust with oversight bodies.

Benefits for Medical Device Manufacturers

- **Streamlined Compliance:**
  Automated security attestations and evidence-based reporting reduce manual effort, enabling manufacturers to focus on innovation while maintaining regulatory compliance.

- **Enhanced Security Posture:**
  Continuous monitoring and proactive risk management ensure that vulnerabilities are addressed before they escalate into serious threats.

- **Operational Efficiency:**
  Embedded security controls in DevOps pipelines accelerate development cycles without compromising on security standards.

- **Regulatory Confidence:**
  Comprehensive, machine-readable documentation builds confidence with regulators, simplifying audits and facilitating smoother market approvals.

Summary

The FDA's Cybersecurity in Medical Devices Guidelines demand a robust, integrated approach to securing software across the entire development lifecycle. Scribe Security's platform meets these requirements by automating security attestations, providing comprehensive visibility into the software supply chain, and embedding security controls directly into DevOps processes. By leveraging Scribe, medical device manufacturers can not only achieve compliance with FDA guidelines but also enhance the overall security and resilience of their products—ensuring safer outcomes for patients and stronger confidence from regulators.

For further information, see https://scribesecurity.com/