Cybersecurity for Medical Devices:

HOW FDA DRAFT GUIDANCE WILL BENEFIT MANUFACTURERS

By Mariano A. Mattei, Vice President of Cybersecurity, Azzur Group

AZZUR GROUP

Table of Contents

Introduction

The FDA issued draft guidance that will change cybersecurity considerations and pre-market submission content for medical device manufacturers, Device Software Functions – Software in a Medical Device (SiMD) and Software as a Medical Device (SaMD), Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions.

Full details can be found in the following guidelines released by the FDA:

- "Content of Premarket Submissions for Device Software Functions, Draft Guidance for Industry and Food and Drug Administration Staff" (November 2021),
- "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions" (April 2022),
- "Postmarket Management of Cybersecurity in Medical Devices" (March 2020),
- "Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices Under Section 524B of the FD&C Act" (March 2023)

SCOPE

The scope of the FDA Draft Guidance covers:

1. Firmware and software-based control of medical devices
2. Stand-alone software applications
3. Software intended to run on general-purpose platforms
4. Dedicated hardware/software medical devices
5. Accessories to medical devices when composed of software

The FDA Draft Guidance applies to all premarket submissions:

1. Premarket Notification (510(k))
2. De Novo Classification Request
3. Premarket Approval Application (PMA)
4. Investigational Device Exemption (IDE)
5. Humanitarian Device Exemption (HDE)
6. Biologics License Application (BLA)

Documentation Level

The FDA will consider four risk-based factors to help determine the Documentation Level.

BASIC DOCUMENTATION

This should be provided for any premarket submission that includes device software function where enhanced documentation does not apply.

ENHANCED DOCUMENTATION

This should be provided for any premarket submission that meets the following requirements:

1. Device is a constituent part of a combination product
2. The device is:
    - A. Intended to test blood donations for transfusion-transmitted infections
    - B. Used to determine donor and recipient compatibility
    - C. A Blood Establishment Computer Software
3. The device is classified as class III
4. A failure or flaw could result in a probable risk of death or serious injury

Documentation Level Cont.

Table 1. Outline of Recommended Documentation (FDA, FDA, 2021)

SOFTWARE DOCUMENTATION ELEMENTS	BASIC DOCUMENTATION	ENHANCED DOCUMENTATION
Documentation Level Evaluation	A statement indicating documentation level and rationale.	
Software Description	Description including features, analysis, inputs, and outputs.	
Architecture Design	Detailed diagrams of modules, layers, interfaces, relationships, inputs/outputs and data flow diagrams, and interfaces.	
Risk Management File	Risk management plan and assessment, mitigation, and report.	
Software Requirements	Complete documentation on needs and expectations of software with traceability of all other documentation.	
Software Design Specification	NONE	Complete documentation in plain language so FDA can understand all data flow and elements of the design.
Software Development & Maintenance	Declaration of Conformity to IEC 62304 **OR** Summary life cycle of configuration management and maintenance activities.	Declaration of Conformity to IEC 62304 **OR** Summary life cycle of configuration plus complete management and maintenance plan documentation.
Revision Level History	Revision history table with all major changes, including date, version, description, relation to previous version, and which version testing was performed.	
Unresolved Anomalies	List of all remaining bugs, defects, and anomalies annotated with descriptions of impact on safety or effectiveness with human factors, workarounds, and timeframe for corrections.	

The CIA Triad

From a Cybersecurity Standpoint, there are three major functions to consider:

CONFIDENTIALITY
INTEGRITY
AVAILABILITY

CONFIDENTIALITY

Prevent unauthorized access to data and/or systems

INTEGRITY

Prevent unauthorized changes or the realizability of information

AVAILABILITY

Ensure timely access to information and resources

The FDA's security objectives add:

1. Authenticity, which includes integrity
2. Authorization
3. Secure and timely updatability and patchability

This is accomplished via a Secure Product Development Lifecycle (SPDL) to satisfy the Quality System Regulation (QSR) requirements in 21 CFR Part 820. (FDA, FDA, 2022)

The SPDL contents will depend on:

1. Intended Use
2. Functionality of Device Interfaces
3. Intended & Actual Operating Environment
4. Types of Vulnerabilities Present
5. Exploitability of the Vulnerabilities
6. Risk to Patient Harm due to Exploitability

The SPDL benefit is security by design whereby exploitability is reduced in combination with vulnerability reduction with failure modes for systems resulting in reduction of risk to patient harm.

Recommended Documentation

More often in today's digital age, the frequency of electronic data of medical device related information, along with the increase in network and interconnected devices, including wireless, has prompted the FDA to update its cybersecurity guidelines in an effort to assure both medical device functionality and patient safety.

The EU, as well as the current US White House Administration, is placing more focus on cyber-maturity and resiliency calling on companies to focus on cybersecurity at every stage of development. With these changes in guidelines, we have several new and mandatory documentation requirements.

Let's take a closer look at the FDA Draft Guidance changes and what that means in terms of recommended documentation

Software Description

An overall operational description of features, that includes images, flow charts, state diagrams, data flow diagrams, and connectivity that adequately describes the intended functionality within the intended environment. These should be in plain language as to be understood by the average user and operator.

Stride

One common Threat Model was developed by Microsoft, called STRIDE. It is a mnemonic device for six security threats in the following categories:

Spoofing
Tampering
Repudiation
Information Disclosure
Denial of Service
Elevation of Privilege

Threat Model

The requirements are described in the Content of Premarket Submission for Management of Cybersecurity in Medical Devices and the Playbook for Threat Modeling Medical Devices. Threat models intend to identify cybersecurity threats and are part of the Cybersecurity Risk Management Process.

DREAD

DREAD is part of a system for risk scoring similar to the Common Vulnerability Scoring System (CVSS), but it provides a less detailed image of the vulnerability and risk. Each threat model must include diagrams that list all assets and connected devices, communication and dataflows, potential risk actors, threats, and defined trust boundaries.

Trust Boundaries are assumptions you can make about the system and internal trustworthiness of interactions. For example, communications may not be dependent upon the network in which the data is transferred.

Cybersecurity Risk Assessment

Risk assessments consider cybersecurity vulnerabilities, defects, and exploits impacting Patient Safety as well as the Confidentiality, Integrity, Availability, and Privacy of the patient data.

For each potential risk factor, a mitigation control and/or compensating controls are listed which will further reduce the risk levels to appropriate levels of acceptance.

Risk Assessment Methodologies

Popular risk assessment methodologies include:

1. NIST SP 800-30
2. IEC 62304
3. ISO 14971
4. MITRE's Medical Device CVSS Rubric

In addition to the risk assessment, documentation regarding security requirements, traceability matrices, device hazard analyses, and penetration testing should also be included.

Cybersecurity Testing

Specific cybersecurity testing must be conducted against the device and all related systems. Types of testing to be conducted include network enumeration to define all devices reachable from a network, open ports, versioning, and OS fingerprinting. Penetration testing must be conducted to eavesdrop on network communication in order to actively insert, modify, drop, or jam network communications.

SAST

Static Application Security Testing (SAST) is a secure code analysis making use of both peer reviews of code and testing tools to automate the detection and testing of top application vulnerabilities.

DAST

Dynamic Application Security Testing (DAST) intentionally attempts known methods of manipulating software functionality for unintended access and use.

DDoS and Performance Testing

Distributed Denial of Service (DDoS) and performance testing is conducted to place the network under an artificial or malicious load that could prevent, hinder, or delay normal communications.

Cybersecurity Risk Assessment Cont.

Fuzzing

Fuzzing is a Dynamic Analysis Technique to provide random, unexpected, or invalid inputs into running software to gain access to unintentional areas of memory or executing malicious code.

SBOM

Software Bill of Materials (SBOM) is a machine-readable listing of all components of software. This detailed list of the entire software supply chain components, libraries, tools, and processes is used to develop, build, and publish software. The SBOM can then be used to scan for known vulnerabilities based on the Common Vulnerability and Exposures (CVE) databases.

Cybersecurity Monitoring

Logging functionality with auditing is required to detect, monitor, log, and alert on all behavior to provide the opportunity to analyze execution for malicious intent.

IDS

Intrusion Detection System (IDS) monitors and detects suspicious activities and generates alerts for further investigation.

IPS

Intrusion Prevention System (IPS) is similar in functionality to IDS with the added benefit of taking immediate action to prevent further malicious actions.

SIEM

Security Information and Event Management (SIEM) is a system by which a Security Operations Center (SOC) can run 24/7/365 as a single source of visibility into all suspected activity, alerts, and events that require further investigation.

SOAR

Security Orchestration, Automation, and Response (SOAR) is like a SIEM with the added benefit of automation playbooks that will act on specific events. SOAR leverages both human and Artificial Intelligence (AI) and Machine Learning (ML) to immediately act against patterned behavior that is known to be malicious.

Cybersecurity Risk Assessment Cont.

Cybersecurity Plan

A cybersecurity plan will include your threat model, cybersecurity risk assessment, and testing procedures. It will also account for the additional policies and procedures required for continuous software vulnerability analysis, incident response, disaster recovery, and business continuity. In addition, specific software patching and updating procedures, including the ability to test and validate updates and patches prior to entering production, is included in the plan. Rollback to previous versions for continued operation is recommended.

Device Configuration, Labeling, and Deployment

All users must have access to clear labeling and documentation on the devices operating, configuration, for the strictest cybersecurity settings with the most robust security. It is preferable that users can not circumvent these most secure settings thereby eliminating the potential risk of misconfiguration resulting in unintentional harm.

Encryption and Security Models

List all risk assessments for Off the Shelf (OTS(S)) software and Software of Unknown Provenance (SOUPs) and provide a rationale if you decide not to update immediately. Each vulnerability, while typically is scored via the CVSS scoring system, should be evaluated independently for the specific device and environment to better determine a risk level and mitigation strategy.

- Only use TLS 1.3 or TLS 1.2 with cipher suites that use Authenticated Encryption with Associated Data (AEAD) for bulk encryption. See RFC 8446.
- Digitally sign and verify software updates using FIPS 140-3 approved algorithms. For example, ECDSA. See FIPS 140-3 or NIST SP 800-140C.
- Enforce server-side access controls for authentication and authorization making use of the principle of least privilege.
- Validate all cloud-based security functionality and refer to the split responsibility diagrams to better understand where the cybersecurity responsibilities reside.
- Mandate encryption at rest wherever possible or provide compensating controls for encryption, such as table level encryption for data.
- Use hardware security modules and critical management services on the backend where possible.
- Do not hardcode any password, credential, secret, API key, etc.
- Employ Zero Trust Architecture Concepts where possible.

Opinion

While it may seem daunting at first glance, the FDA Draft Cybersecurity recommendations bring medical device manufacturers more inline with DevSecOps than DevOps.

Cybersecurity cannot be bolted on afterwards but must become part of the DNA of the process of manufacturing medical devices and accompanying software. During each phase of the MDM process, cybersecurity considerations will be documented, resulting in reduced risk and increased safety for patients.

By adopting early, Medical Device Manufacturers can not only increase security of their devices, but also ensure compliance which will prevent lengthy delays, which:

- ✓ **Reduces their liability**
- ✓ **Improves the brand’s reputation**
- ✓ **Ultimately makes safer devices for their patients**

Change is coming, and it’s good.

Conclusion

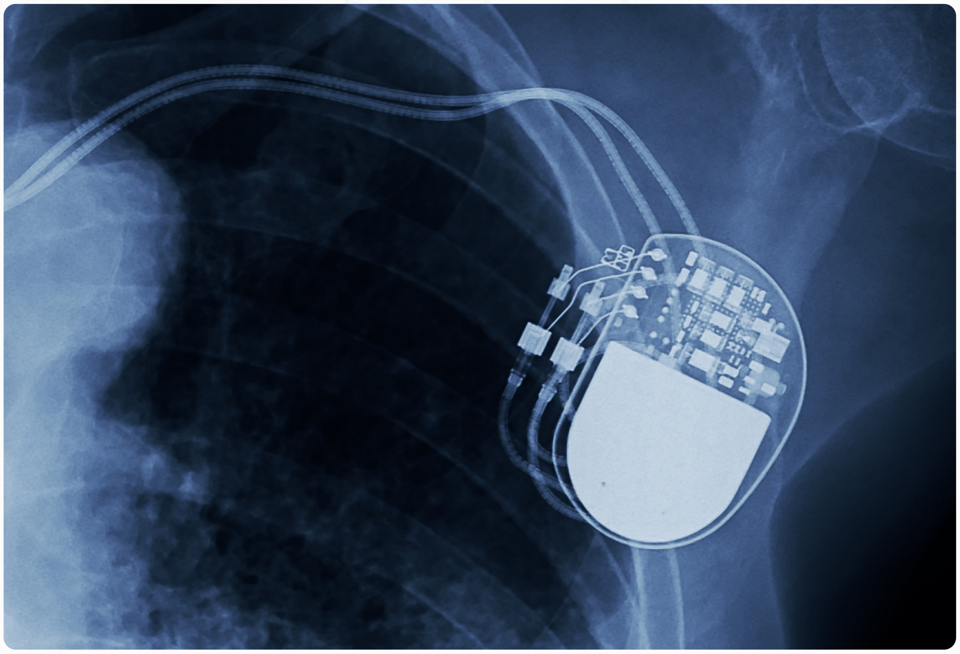
The request for comments for the “Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff” closed in July of 2022.

The hope is that when the final guidance is released, all the benefits from a well thought out action plan for increased cybersecurity in medical devices will be included.

FBI’s Most Vulnerable Medical Devices

The FBI White Notice dated September 12, 2022, PIN Number 20220912-001, released the most vulnerable medical devices as noted below. (FBI, 2022)

- **Insulin Pumps**
- **Intracardiac Defibrillators**
- **Mobile Cardiac Telemetry**
- **Pacemakers**
- **Intrathecal Pain Pumps**



About the Author: Mariano A. Mattei

Mariano A. Mattei is the Vice President of Cybersecurity and CISO for Azzur Group. With over 30 years of experience as a Software Developer, Global Solutions Manager, and Cybersecurity Professional, he is considered a Cybersecurity Subject Matter Expert in QA, IT, Manufacturing, Operations, Clinical, and R&D in FDA-Regulated Environments.

Currently holding a EC-Council Certified Chief Information Officer Certification, he is pursuing a master’s in Cybersecurity and Data Assurance at Temple University where he obtained his bachelor’s in Computer and Information Science.

About Azzur Group

From Discovery to DeliveryTM, Azzur Group provides the life science community full life-cycle solutions for all of their GxP needs.

From Azzur Cleanrooms on DemandTM facilities, to our labs, training centers and consulting offices across the nation, Azzur Group helps organizations start, scale, and sustain their growing enterprises. With nearly four decades of service to the life science community, we have become a trusted partner to the world's leading pharmaceutical, biotechnology, medical device, and healthcare companies, as well as their supply chain.

For more resources on this topic, or to learn about solutions Azzur Group provides to organizations in the life science community visit: azzur.com/services/it-advisory-services.

References

FBI. (2022, September 12). FBI. Retrieved from Upatched and Outdated Medical Defvices provide Cyber Attack Opportunities: https://www.aha.org/system/files/media/file/2022/09/fbi-pin-tlp-white-unpatched-and-outdated-medical-devices-provide-cyber-attack-opportunities-sept-12-2022.pdf

FDA. (2021, November 04). FDA. Retrieved from Content of Premarket Submissions for Device Software Functions - Draft Guidance: https://www.fda.gov/media/153781/download

FDA. (2022, November 29). FDA. Retrieved from CFR - Code of Federal Regulations Title 21: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=820

FDA. (2022, April 08). FDA. Retrieved from Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions - Draft Guidance: https://www.fda.gov/media/119933/download