Welcome To Today's Webinar

Thanks for joining us!
We'll get started in a few minutes

Today's Topic:

Draft Guidance on Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

June 14, 2022

Draft Guidance:
Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Matthew Hazelett
Cybersecurity Policy Analyst
Clinical and Scientific Policy Staff
Office of Product Evaluation and Quality
Center for Devices and Radiological Health
U.S. Food and Drug Administration

Draft Guidance

- **Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions**
  - www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions

A Note about Draft Guidance

- You may comment on any guidance at any time
  - see 21 CFR 10.115(g)(5)
- Please submit comments on draft guidance before closure date
  - to ensure that FDA considers your comment on the draft guidance before we work on final guidance
- This is a draft guidance. The recommendations discussed today are proposals and may change based on public comment.

Learning Objectives

- Describe the updates from the 2018 draft
- Describe the general principles proposed in the guidance
- Describe the proposed design and documentation recommendations
- Describe the proposed transparency recommendations

Updates From the 2018 Draft

Guidance Title Change

- Reflects expanded scope of guidance and the increased focus on how cybersecurity fits into Quality System (QS) Regulation
- Provides greater detail from 2014 Final Premarket Guidance on how FDA recommends cybersecurity be incorporated in device design and Total Product Lifecycle (TPLC) maintenance
- Outlines how QS Regulation aligns with the Secure Product Development Framework (SPDF)
- Highlights importance of QS Regulation integration as some medical device manufacturers (MDMs) have not fully incorporated cybersecurity into their quality systems

Content Differences

- **Expanded scope**
  - Provides more detail how cybersecurity aligns with the QS Regulation
  - Recommends assessment of system, not just end device in isolation to ensure all the relevant cybersecurity risks are appropriately addressed by the end-device design
- **Alignment with SPDF**
  - SPDFs exist as best practices within medical device sector and other sectors
- **Removed risk tiers for devices**
  - Based on public comments and to encourage all manufacturers to appropriately consider cybersecurity risks

Content Differences (cont.)

- **Changed Cybersecurity Bill of Materials (CBOM) to Software Bill of Materials (SBOM)**
  - Alignment with industry/sector efforts
  - Alignment with Presidential Executive Order 14028
- **More detailed recommendations for premarket submission documentation**
  - Increase clarity on documentation recommendations to help improve review process
- **Added Investigation Device Exemptions (IDEs) to scope with a subset of documentation recommendations**
  - Both to ensure cybersecurity is designed into the device and ensure patients are informed of cybersecurity risks for the devices

Proposed Scope

- **This guidance document is applicable to devices that contain software (including firmware) or programmable logic, as well as software as a medical device (SaMD).**
  - Devices within the meaning of section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C Act) whether or not they require a premarket submission.
  - The guidance is not limited to devices that are network-enabled or contain other connected capabilities.

Proposed Scope (cont.)

- **Applicable Submission Types:**
  - Premarket Notification (510(k)) submissions
  - De Novo requests
  - Premarket Approval Applications (PMAs) and PMA supplements
  - Product Development Protocols (PDPs)
  - Investigational Device Exemption (IDE) submissions
  - Humanitarian Device Exemption (HDE) submissions

Proposed General Principles

Proposed General Principles A&B

A. Cybersecurity is Part of Device Safety and the QS Regulation

- Cybersecurity is a part of safety and effectiveness
- Cybersecurity aligns with the QS Regulation
- A SPDF can be used to fulfill aspects of QS Regulation

B. Designing for Security

- “Design in” rather than “bolt on” cybersecurity controls
- Outlines key security objectives medical devices should achieve

Proposed General Principles C&D

C. Transparency

- Importance of end user having cybersecurity information to ensure continued safe use of the device

D. Submission Documentation

- Recommendations complement and are in addition to the software premarket guidance
- Documentation expected to scale with cybersecurity risk of device

Proposed Design and Documentation Recommendations

Proposed Design Recommendations

- **Security Objectives for Design:**
  - Authenticity, which includes integrity
  - Authorization
  - Availability
  - Confidentiality
  - Secure and timely updateability and patchability

Proposed Design Recommendations

- 8 Security Control Categories to help in meeting the Security Objectives
- Appendix 1 provides specific control recommendations and implementation guidance for consideration to avoid common pitfalls
- Appendices are part of the document recommendations

Proposed Documentation Recommendations

- **Section V. Using an SPDF to Manage Cybersecurity Risks**
  - A. Security Risk Management
  - B. Security Architecture
  - C. Cybersecurity Testing
- **Section VI. Cybersecurity Transparency**
  - A. Labeling Recommendations
  - B. Vulnerability Management Plans

Proposed Security Risk Management

- System-level assessment
- Security risk management distinct from safety risk management but the two processes should feed into and out of one another
- Use of exploitability assessment for security risks
  - Premarket exploitability assessment may differ from postmarket assessments
- Known vulnerabilities should be assessed as reasonably foreseeable
- Risk transfer should only occur if all relevant information is known, assessed, and communicated to users

Proposed Security Risk Management (cont.)

1. **Threat Modeling**
   - Includes full system and lifecycle of the device
2. **Third Party Software Components**
   - SBOM and vulnerability assessment
3. **Security Assessment of Unresolved Anomalies**
   - Anomalies can present a different vector to safety risks through cybersecurity
4. **Security Risk Management Documentation**
   - Security Risk Management Plan and Report
5. **TPLC Security Risk Management**
   - Maintain resources and documentation
   - Track and monitor cybersecurity measures and metrics

Proposed Software Bill of Materials (SBOM)

- **Recommended Elements:**
  A. The asset(s) where the software component resides
  B. The software component name
  C. The software component version
  D. The software component manufacturer
  E. The software level of support provided through monitoring and maintenance from the software component manufacturer
  F. The software component's end-of-support date
  G. Any known vulnerabilities

Proposed SBOM (cont.)

- Industry-accepted formats of SBOMs can be used to provide this information to FDA; however, if any of the [above] elements are not captured in such an SBOM, we recommend that those items also be provided, typically as an addendum, to FDA for the purposes of supporting premarket submission review.

- SBOMs provided to users in labeling can conform with industry-accepted formats

Proposed Architecture Views

- Can be part of Threat Modeling Documentation
- 4 View Categories
    a) Global System View
    b) Multi-Patient Harm View
    c) Updateability/Patchability View
    d) Security Use Case View(s)
        – Operational states and different clinical use cases

Proposed Architecture Views

- These security architecture views should:
  - Identify security-relevant system elements and their interfaces;
  - Define security context, domains, boundaries, and external interfaces of the system;
  - Align the architecture with (a) the system security objectives and requirements, (b) security design characteristics; and
  - Establish traceability of architecture elements to user and system security requirements.

- Level of recommended detail for the architecture views captured in Appendix 2 including:
  - Call-Flow Diagrams
  - Information Details for an Architecture View

Proposed Testing

- Recommendations on Types of Testing:
  - Security Requirement Testing
  - Threat Mitigation
  - Vulnerability Testing
  - Penetration Testing

- Section also makes recommendations on:
  - Independence and technical expertise of testers
  - Scope of testing (i.e., system-level)
  - Third-Party Testing recommendations
  - Submission documentation

Proposed Transparency: Labeling and Vulnerability Management Recommendations

Proposed Labeling Recommendations

- Largely similar to recommendations provided in 2018 Draft with some changes and reordering
- Can be provided in different locations depending on appropriate users for the information (manual vs. security implementation guide)
- Labeling mitigations and risk transfer items may need to be included as part of Human Factors Testing tasks
- Focus on ensuring users have sufficient information on device to integrate it and have sufficient information to manage security risks and updates

Proposed Vulnerability Management Plans

- Recommendations expand on the plan for providing validated software updates and patches described in the 2014 Premarket Guidance
- Plans should include Coordinated Vulnerability Disclosure process as described in the 2016 Postmarket Guidance
- Also includes items like:
  - Periodic security testing to test identified vulnerability impact
  - Timeline to develop and release patches
  - Patching capability (i.e., rate at which updates can be delivered to devices)

Resources

Slide Number	Cited Resource	URL
6, 27	2014 Premarket Guidance: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices	www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices
13	Premarket Software Guidance: Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices	www.fda.gov/regulatory-information/search-fda-guidance-documents/guidance-content-premarket-submissions-software-contained-medical-devices
27	2016 Postmarket Guidance: Postmarket Management of Cybersecurity in Medical Devices	www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

Submit Comments to Docket by: July 7, 2022

- **Draft Guidance: Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions**
  - Docket: FDA-2021-D-1158 (www.regulations.gov/document/FDA-2021-D-1158-0001)
  - Guidance

Summary

- This draft is more detailed than the 2018 Draft
- The general principles proposed in Section IV outline the core concepts in the guidance
- The proposed design recommendations focus on security objectives and that documentation will scale with cybersecurity risk
- Transparency of device cybersecurity recommendations include proposals for proactive labeling and plans to respond to emerging issues throughout the TPLC


FDA
U.S. FOOD & DRUG
ADMINISTRATION

Additional Panelists

Linda Ricci

Division Director
Division of All Hazards Response, Science and Strategic Partnerships
Office of Strategic Partnerships and Technology Innovation
Center for Devices and Radiological Health
U.S. Food and Drug Administration

Aftin Ross

Senior Special Advisor for Emerging Initiatives
Office of Strategic Partnerships and Technology Innovation
Center for Devices and Radiological Health
U.S. Food and Drug Administration

Let's Take Your Questions

- **To Ask a Question:**
  1. Please "Raise Your Hand" 

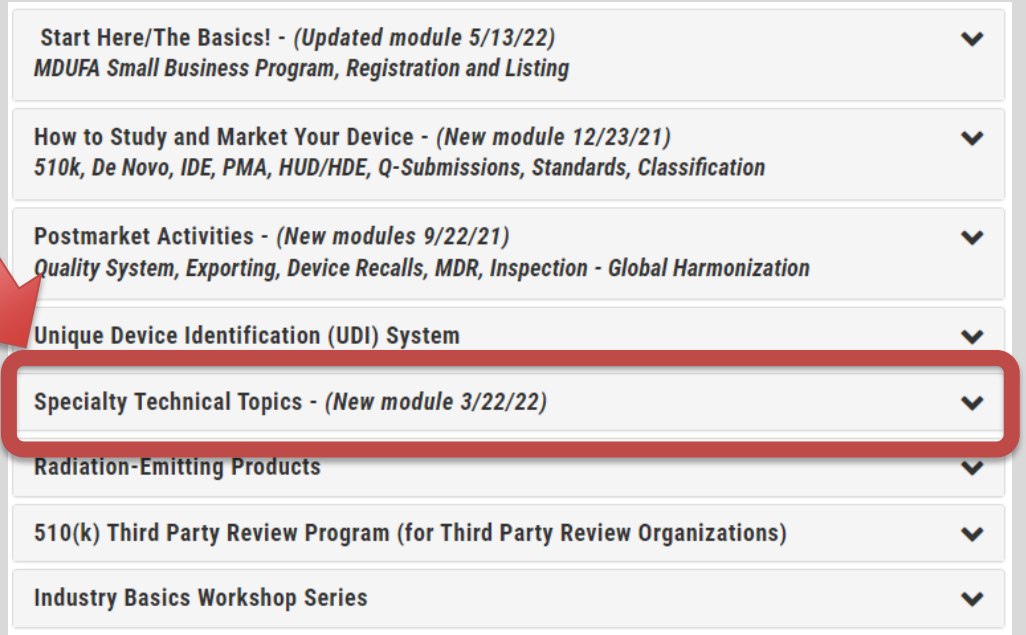
  2. Moderator will Announce Your Name to Invite You to Ask Your Question
  3. Unmute yourself when called

- **When Asking a Question:**
  - Ask 1 question only
  - Keep question short
  - No questions about individual submissions

- **After Question is Answered:**
  - Please mute yourself again
  - If you have more questions - raise your hand again

Thanks for Joining Today!

- **Presentation and Transcript will be available at CDRH Learn**
  - www.fda.gov/Training/CDRHLearn
- **Additional questions about today's presentation**
  - Email: DICE@fda.hhs.gov
- **Upcoming Webinars**
  - www.fda.gov/CDRHWebinar




FDA
U.S. FOOD & DRUG
ADMINISTRATION