MCRA
A Full-Service Integrated CRO & Advisory Firm

MCRA Overview: 2022 FDA Draft Guidance

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

High Level Overview:

Over the years, we have continued to see an increase in cyber security threats that put organizations and their data at risk. With the threat landscape increasing, it's imperative that companies begin to look at security holistically by integrating security into the organization's culture and subsequently into the products or solutions they are delivering.

What the FDA has done with this guidance is emphasize the need to bring security into a company's business model. By integrating security into quality management systems and broadening the scope of their guidance to create a more robust approach to cybersecurity with medical devices, it shows they are starting to acknowledge its importance.

That's the good news, but what does this mean as a future state for FDA review? In our experience, FDA reviewers lack the technical expertise to properly execute cybersecurity and software review but recognize the need for a more robust process. This will come with time, but we expect to see inconsistencies in device reviews as they move this forward. To that point, we have put together a high-level review of key changes in the draft guidance and our thoughts on those changes.

Key Considerations:

- ***Expanded Scope:***
    - Scope has expanded from previous draft guidance to include a more detailed approach on how cybersecurity should align with quality system regulations.
        - Addresses how cybersecurity is part of the safety and effectiveness of a device.
    - Focus should be to look at security holistically encompassing the whole system and not just end-device design. This means incorporating security by design through secure software development lifecycle (sSDLC) practices.

        - Designing for security ensures that security is built into the device design instead of being bolted on at the end. It also outlines key security objectives medical devices should achieve.
            - Key Objectives include:
                - Authenticity to include integrity
                - Authorization
                - Availability
                - Confidentiality
                - Secure and timely updates and patches to the system.
    - Investigation device exemptions (IDE's) have been added to the scope of FDA review and a new subset of documents have been included. This is to ensure cybersecurity is designed into the device and ensure patients are informed of security risks for the device.
    - Additional appendices added for security control categories, details for security architecture flows, submission documentation for IDE's and terminology.
    - 9 pages (2014) to 45 (2022) pages of guidance documentation.

- ***Removal of Risk Tiers for Devices***
    - By removing risk tiers, it encourages ALL manufacturers to appropriately consider cybersecurity risks for their device(s).

- ***Changed Cybersecurity Bill of Materials (CBOM) to Software Bill of Materials (SBOM)***
    - This is in alignment with industry best practices and with Presidential Executive Order 14028.
    - You will likely find this requirement burdensome and very FDA-centric in ask. Post-FDA approval you'll also want to look into providing the MDS2 to clinics or hospitals looking to adopt your device.

- ***Detailed recommendations for premarket submission documentation***
    - Increased clarity on documentation recommendations to improve FDA's review process.

- ***Using SPDF or Secure product development lifecycle (also known as secure software development lifecycle) to better manage security risks.***
    - Security Risk Management
        - Unresolved anomalies – This looks to be a Yes/No column in the UA table indicating those that are of cyber risk. Anything documented as "yes" would need a follow up assessment.
        - TPLC Security risk management- There is some redundancy here but there is an emphasis on having a plan documented as part of you QMS.
    - Security Architecture Views
        - 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 the user and system security requirements.
        - Line 600 talks about requirements with an acceptance criterion and design processes for security considerations. This would normally be included in your software documentation so navigating this both from a documentation standpoint and that of the FDA could be a challenge.
    - Security Testing – This section of the documentation does include recommendations on the independence and expertise of testers, scope of testing, third-party recommendations, and submission documentation expected.
        - Security Requirement Testing
        - Threat Mitigation
        - Vulnerability Testing
        - Penetration Testing
    - Labeling Recommendations
        - Similar to 2018 draft guidance.
        - Emphasis on transparency; meaning there will be a shift in focus on end-user labeling and communication on how updates for cybersecurity are completed (see CVD below).
        - Draft guidance for labeling starts on line 931 and should be implemented sooner than later.
    - Vulnerability Management Plans
        - Expanded on 2014 guidance to include coordinated vulnerability disclosure as seen in 2016 post market guidance.

- Includes periodic security testing to test identified vulnerability impact.
- Timelines to develop and release patches.
- Patching capability i.e. the rate at which updates can be delivered.