How to Avoid Pitfalls When Planning an FDA Submission

Post Webinar Q&A

Q: Can you discuss legacy devices in the context of cybersecurity? How should we remediate them to ensure compliance?
A: Managing legacy devices that cannot be updated or changed is a challenging situation, often stemming from gaps in the initial development process. The most effective approach is to bring the device up to date with the latest operating systems and software. This proactive strategy is typically more straightforward than justifying to the FDA why updates can't be made, as valid reasons for non-compliance are rare. Create and maintain a Software Bill of Materials (SBOM) for legacy devices. Even if the device itself cannot be modified, an SBOM can help identify and track potential vulnerabilities, allowing for targeted mitigation efforts or planning for future device replacement.

Q: Is the "internet" also an app downloaded from Apple or Google app store?
A: If an app is a core part of the medical device's functionality, such as providing the only means to view essential data (e.g., SpO_2 and pulse rate for a pulse oximeter ring), it is considered part of the device itself. In such cases, the app requires cybersecurity documentation. This ensures that all components of the device, including the app, meet the stringent cybersecurity standards expected by the FDA.

Q: How does sharing this information with the FDA work in the context of PCCP and AI-ML enabled devices?
A: When it comes to sharing information on predetermined change-control plans (PCCP) for AI/ML solutions, it's crucial to adhere to the current draft guidance provided by the FDA. While this is still a draft and subject to change, aligning with it now sets a strong foundation for future compliance. For finalized guidance, the FDA's software guidance, particularly section VI.B (page 13, last bullet point), should be your primary reference. Staying ahead of these evolving requirements is key to ensuring a smooth submission process.

Q: What criteria can we use to determine if our device needs a penetration test?
A: Penetration testing is a requirement for all cyber devices, regardless of their complexity. Even for devices with limited communication capabilities, a pen test is necessary. While it may be a simpler process for such devices, ensuring that this step is completed is critical to meet FDA cybersecurity expectations.

Q: What are your thoughts on using accreditation labs to certify the cybersecurity of devices, akin to third-party certification?
A: Third-party certification of cybersecurity by accredited labs could play an important role in enhancing device security, particularly in regulated industries like healthcare, where patient safety is paramount. However, it is important that such certifications be part of a larger, continuous cybersecurity strategy that includes ongoing monitoring, patch management, and incident response.

Q: The FDA guidance on cybersecurity (Sep 2023) includes recommendations that exceed the requirements of recognized consensus standards. What approach do you recommend to cover these additional requirements?
A: When it comes to compliance, FDA guidance should always take precedence over consensus standards. To ensure full compliance, it's best to provide all the information requested by the guidance, even if it goes beyond the recognized standards. This approach not only aligns with regulatory expectations but also strengthens the overall security posture of your device.

Q: Would a lack of third-party penetration testing cause the FDA to issue a "Refuse to Accept"? What other cybersecurity testing or validation does the FDA look for or recommend?
A: In the eSTAR process, a "Refuse to Accept" (RTA) has largely been replaced by Technical Screening -- Incomplete (TSIC). Both RTA and Technical Screening (TS) are primarily document completeness checks. While a missing penetration test report should be flagged during TS, it's possible, though not ideal, to pass TS without one. To avoid potential delays or rejections, ensure all cybersecurity documentation, including penetration test reports, is complete and accurate.

Q: How do the requirements for a predicate device submission differ?
A: Assuming this pertains to cybersecurity requirements, if you have an existing predicate device that was cleared before the implementation of section 524B, the cybersecurity documentation was likely minimal or nonexistent. When submitting a new 510(k) for a device that introduces a clinical feature without impacting cybersecurity, full CS documentation is now required according to the 2023 guidance. The FDA may deny clearance if the device does not meet current cybersecurity standards.

Q: Do you need to notify customers of vulnerabilities, existing or patched, for a software medical device delivered in a SaaS platform? If so, how?
A: Yes, customers must be informed of any existing or newly discovered vulnerabilities, even for Software as a Medical Device (SaMD) delivered via SaaS. The method of communication should be clearly outlined in your Cybersecurity Management Plan. This plan should include how you intend to notify customers about forthcoming patches, updates, and remediation efforts to ensure they are aware of the device's security status.

Q: The FDA guidance requires non-standard fields outside CycloneDx, SPDX, and SWID, such as the level of support and end-of-support for each software component. How do you recommend capturing these details, and are there tools that consider them?
A: Providing end-of-support dates for operating systems and commercial software components is generally sufficient. For open-source components, stating that support is provided by the open-source community without a specific end date is acceptable. The FDA typically accepts this approach, especially when all information for addressing vulnerabilities is available in public repositories. In order to include more detailed information, public sources are available for manual searching, such as https://endoflife.date/, however there are a small number of tools that can make reporting this data much less cumbersome. For example, Vigilant Ops provides a streamlined way to get this information right into the SBOM. For completeness, extended maintenance contracts should be included in the documentation to further support the submission.

If you have any further questions or need personalized guidance, don't hesitate to reach out to our team. We're here to support you every step of the way.
www.vigilant-ops.com