Improve Cybersecurity in Medical Devices and Navigate FDA Guidance with Mayhem

Mayhem

What is the FDA Cybersecurity Guidance for Medical Devices?

The FDA guidance "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions", released September 25, 2023, provides recommendations on medical device cybersecurity and what information to include in premarket submissions.

Why is the FDA Guidance for Medical Devices Needed?

The FDA's guidance highlights several examples of cybersecurity threats to medical devices, including the 2017 WannaCry ransomware attack that impacted global hospitals and medical tools, vulnerabilities in widely used third-party components like URGENT/11 and SweynTooth, and the 2020 German hospital attack causing patient care disruptions.

These events show that different areas of medicine and healthcare are at risk, as is patient safety. As more medical devices connect wirelessly and share information electronically, it becomes increasingly important to make sure they are safe from cyber attacks.

The FDA guidance stresses the need for better cybersecurity to deal with the changing threats. The goal of the guidance is to make sure medical devices are secure from the beginning to the end of their use, and it highlights the importance of designing them securely and having mitigation strategies in place.

How Does the Guidance Affect Device Manufacturers and Development Teams?

The FDA guidance applies to a wide range of stakeholders involved in the development and regulatory processes of medical devices. The guidance recommends the following measures for device manufacturers:

- Integrate cybersecurity measures early using a Secure Product Development Framework (SPDF).
- Provide comprehensive documentation and risk assessments, focusing on third-party software components.
- Conduct thorough cybersecurity testing, including penetration and vulnerability testing.
- Maintain detailed testing records of testing results for premarket submissions to ensure device safety and effectiveness.
- Address known vulnerabilities through safety and security risk assessments.
- Adopt Software Bill of Materials (SBOM) practices to identify devices affected by known vulnerabilities.

By adhering to these recommendations, manufacturers can enhance the cybersecurity posture of their medical devices and demonstrate compliance with regulatory guidelines.

Using Mayhem to Address Key Areas of the FDA Guidance

Teams developing software for medical devices can use Mayhem to aid compliance with the FDA Guidance. The Mayhem platform makes it easy for teams to perform dynamic testing and assess risk status of vulnerabilities. Mayhem covers all layers of the application, from custom code to third party components.

#	Section	Control	How Mayhem Helps
V A.4	Third-Party Software Components	As part of demonstrating compliance with design controls under 21 CFR 820.30(g), and to support supply chain risk management processes, all software, including those developed by the device manufacturer ("proprietary software") or obtained from third parties, should be assessed for cybersecurity risk. To assist FDA's assessment of the device risks and associated impacts on safety and effectiveness related to cybersecurity, FDA recommends that premarket submissions include SBOM documentation as outlined below. For cyber devices, an SBOM is required (see section 524B(b)(3) of the FD&C Act) For components with known vulnerabilities, device manufacturers should provide in premarket submissions: • A safety and security risk assessment of each known vulnerability (including device and system impacts); and • Details of applicable safety and security risk controls to address the vulnerability. If risk controls include compensating controls, those should be described in an appropriate level of detail.	Mayhem provides a copy/paste reproduction and automatically created regression test for every issue found. With these, developers can replay any defect to support information gathering for remediation.

#	Section	Control	How Mayhem Helps
V A.5	Security Assessment of Unresolved Anomalies	Some anomalies discovered during development or testing may have security implications and may also be considered vulnerabilities. As a part of ensuring a complete security risk assessment under 21 CFR Part 820.30(g), the assessment for impacts to safety and effectiveness may include an assessment for the potential security impacts of anomalies. The assessment should also include consideration of any present Common Weakness Enumeration (CWE) categories. For example, a clinical user may inadvertently reveal the presence of a previously unknown software anomaly during normal use, where the impact of the anomaly might occur sporadically and be assessed to be acceptable from a software risk perspective. Conversely, a threat might seek out these types of anomalies and identify means to exploit them in order to manifest the anomaly's impact continuously, which could significantly impact the acceptability of the risk when compared to an anomaly assessment that didn't include security considerations.	Mayhem's dynamic behavior testing identifies vulnerabilities that are exploitable as threat vectors. Each vulnerability is matched against CWE categories, where appropriate, and guidance on remediation is provided when available.

#	Section	Control	How Mayhem Helps
V A.6	TPLC Security Risk Management	At a minimum, FDA recommends tracking the following measures and metrics or those that provide equivalent information: • Percentage of identified vulnerabilities that are updated or patched (defect density); • Duration from vulnerability identification to when it is updated or patched; and • Duration from when an update or patch is available to complete implementation in devices deployed in the field, to the extent known.	Mayhem tracks the fix rate and time to remediation of all vulnerabilities found.

#	Section	Control	How Mayhem Helps
V C	Cybersecurity Testing	Manufacturers should provide details and evidence of the following testing and analyses: • Abuse or misuse cases, malformed and unexpected inputs; • Robustness. • Fuzz testing. • Attack surface analysis; • Vulnerability chaining; • Closed box testing of known vulnerability scanning; • Software composition analysis of binary executable files; and • Static and dynamic code analysis, including testing for credentials that are "hardcoded," default, easily guessed, and easily compromised.	Mayhem provides easy to export reports/ results of all tests run. Mayhem checks for abuse/misuse cases, malformed and unexpected inputs, and performs fuzz testing. Mayhem's dynamic SBOM performs attack surface analysis and can be used to augment static code analysis or software composition analysis of binary files.

How Mayhem Can Help Medical Device Manufacturers

Though navigating the FDA guidance for cybersecurity in medical devices poses a challenge for medical device manufacturers, complying with the guidance is essential for both regulatory compliance and patient well-being.

Mayhem is a powerful tool in safeguarding against cyber threats, automatically generating tests, addressing vulnerabilities, and enhancing the cybersecurity posture of medical devices. Equip your team with Mayhem to not only meet FDA requirements but to proactively safeguard your connected medical devices.

Get a Demo

Mayhem