Integrating FDA's new cybersecurity guidance into medical device human factors engineering processes

Bold Insight

Kaitlin Stinson

How does a manufacturer ***demonstrate compliance*** with the HFE-related recommendations in this new guidance?

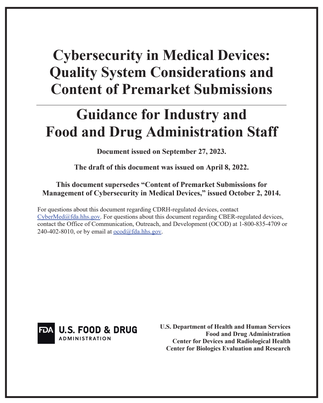
The guidance covers labeling requirements and testing cybersecurity risks but **lacks implementation steps.**

Based on our experience, we recommend integrating the following steps into design controls to ensure compliance.

The steps below follow an ideal early-stage implementation but can be adjusted based on the device's development stage, circumstances, and constraints.

BACKGROUND

Integrating connected medical devices into healthcare introduces cybersecurity risks. The growing use of networked technologies in medical devices highlights the **need for strong cybersecurity to ensure safety and functionality.**



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

Guidance for Industry and Food and Drug Administration Staff

Document issued on September 27, 2023.

The draft of this document was issued on April 8, 2022.

This document supersedes "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," issued October 2, 2014.

For questions about this document regarding CDRH-regulated devices, contact CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010, or by email at ocod@fda.hhs.gov.

U.S. FOOD & DRUG ADMINISTRATION

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

In response, the FDA has issued a final guidance, **Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions**, intended to:

1. Promote consistency
2. Facilitate efficient premarket review
3. Help ensure that marketed medical devices are sufficiently resilient to cybersecurity threats.

In the guidance, the FDA provides recommendations to the industry regarding cybersecurity device design, labeling, testing, and the documentation they recommend be included in premarket submissions for devices with cybersecurity risk.

Fig. 1: Three examples of software-driven medical devices.

Gordon, W.J., Stern, A.D. Challenges and opportunities in software-driven medical devices. Nat Biomed Eng 3, 493–497 (2019). https://doi.org/10.1038/s41551-019-0426-z

This guidance document applies to devices with cybersecurity considerations, including devices with a device software function or that contain software (including firmware) or programmable logic.

1 DESIGN & DEVELOPMENT PLANNING

☐ Risk Management Plan:

Include content in the Risk Management plan that specifies:

- The process to identify use-related cybersecurity risks.
- How to mitigate these risks in, at a minimum, the product's labeling.
- Mitigations must be tested via human factors (HF) methods to ensure their effectiveness.

☐ HFE Plan:

Include content in the HF Plan about:

- The process to ensure use-related cybersecurity risks are identified through the use-related risk analysis (URRA) process.
- How risks will be evaluated via analytical and empirical usability testing methods.
- Which of these risks (i.e., all or only those associated with critical tasks or serious harm) must be tested in HF Summative Validation.

2 DESIGN INPUT

☐ Cybersecurity Risk Assessment:

Identify use-related cybersecurity risks during the Cybersecurity Risk Assessment.

- To help manage traceability and enhance the visibility of adherence to the guidance, employ a categorization scheme to label each risk type to easily identify which risks are use-related and specify the labeling requirement(s) used to mitigate each risk.

☐ Task analysis:

Ensure that task analysis covers all use-related cybersecurity use scenarios, workflows, and tasks associated with device use.

☐ Use/Application FMEA & URRA:

Evaluate use-related cybersecurity risks in the Use/Application Failure Mode and Effects Analysis (FMEA) to ensure adequate mitigation measures are implemented in the user interface's design and labeling. Document these risks in the Use-Related Risk Assessment (URRA).

☐ User interface requirements & specifications:

Develop user interface requirements and specifications with the input of HF team members.

3 DESIGN OUTPUT

☐ User interface design:

Product labeling (e.g., device labels or markings, IFU, training) must be implemented to adequately mitigate use-related cybersecurity risks in addition to other user interface design mitigations implemented based on the output of the u/aFMEA.

The labeling should be designed to communicate to users the relevant device security information so that users can take appropriate actions to manage those types of risks that may enable their ongoing security posture or an organization's overall state of cybersecurity readiness, thereby helping ensure a device remains safe and effective throughout its lifecycle.

To ensure that labeling is implemented effectively, consider the following when developing labeling strategies:

- Review the examples in the guidance document to determine applicability to the medical device under development.
- The depth of detail, the exact location in the labeling for specific types of information (e.g., operator's manual, security implementation guide), and the method to provide this information should account for the intended user of the information (e.g., is the user a patient or caregiver with limited technical knowledge? or is the user a hospital technician with significant technical knowledge and experience?).

☐ Usability test plans/protocols:

Include tasks associated with use-related cybersecurity risks in formative usability studies to ensure risk-mitigating controls are designed effectively, that labeling controls are understandable, and that users have the information they need to take appropriate actions to manage these risks.

4 HF VALIDATION

☐ HF Summative Validation study:

Include use-related cybersecurity critical tasks in the HF Summative Validation study to validate the controls mitigating these types of risks. Performance-based and knowledge-task evaluation methods should include labeling implemented to control for use-related cybersecurity risks.

☐ HFE report:

Document the process used to appropriately identify, mitigate, and test use-related cybersecurity risks during the HFE process throughout the device's development lifecycle in the HFE report.

CONCLUSIONS

Although the FDA's guidance focuses specifically on the recommendation to implement and test labeling controls to mitigate use-related cybersecurity risks, the steps listed above go beyond this type of control strategy to include non-labeling-based controls within the medical device's user interface design.

This recommendation is based on the 2016 FDA HFE guidance document, which indicates that labeling, or information for safety, is the least effective risk mitigation control strategy when used alone and based on HFE best practices. Furthermore, since the FDA has released guidance on this topic, they will likely have use-related cybersecurity risks at the top of their minds when reviewing HF submissions for devices with these types of risks. The plan we've outlined maximizes mitigating these types of risks to reduce them to be as low as possible. Lastly, the approach presented here provides a comprehensive strategy that ensures cybersecurity risk management is embedded into the design-controls process and that human factors engineering is part of the process.