What's changed in the Draft Guidance for Content of Premarket Submissions for Device Software Functions?

Author: Pooja Kartik

Date: January 26, 2022

FDA has released a draft guidance titled "Content of Premarket Submissions for Device Software Functions" as of November 4, 2021, for public comments. When final, this guidance will replace the 2005 guidance document, "Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices. See public comments for the draft at https://www.regulations.gov under docket FDA-2021-D-0775.

The draft guidance reflects FDA's most current thinking on the recommended documentation that companies should include in premarket submissions for FDA's evaluation of the safety and effectiveness of device software functions. It applies to both Software as a Medical Device (SaMD) and Software in Medical Device (SiMD) cases. Further, the guidance applies to all types of premarket submissions for software devices, including:

- Premarket Notification (510(k))
- De Novo Classification Request
- Premarket Approval Application (PMA)
- Investigational Device Exemption (IDE)
- Humanitarian Device Exemption (HDE)
- Biologics License Application (BLA)

This FDA draft guidance is a complete rewrite and it sets out a model of what FDA expects companies to provide in premarket submissions. It is intended to streamline the organization and the content of the software documentation and help with identifying the minimum required elements for the submission.

In an attempt to achieve international harmonization, this draft introduces three new definitions:

1. Device Software Function - Software function that meets the device definition in section 201(h) of the FD&C Act. "Software as a Medical Device (SaMD)" and "Software in a Medical Device (SiMD)" are device software functions. As noted in the FDA draft guidance, the term "function" is a distinct purpose of the product, which could be the intended use or a subset of the intended use of the product.
2. Software as a Medical Device (SaMD) - Software that meets the definition of a device in section 201(h) of the FD&C Act and is intended to be used for one or more medical purposes without being part of a hardware device.

3. Software in a Medical Device (SiMD) - Software that meets the definition of a device in section 201(h) of the FD&C Act, and is used to control a hardware device or is necessary for a hardware device to achieve its intended use. Typically, SiMD is embedded within or is part of a hardware device.

The key change for documentation to be submitted is as follows. The 2005 FDA guidance has three categories—*Minor*, *Moderate* and *Major*—which aid in determining the level of documentation for submission; while the new FDA draft guidance has two categories—*Basic* and *Enhanced*.

In the 2005 FDA guidance, the Level Of Concern assessment starts at *Major* and through the process of elimination it reaches *Minor*. Whereas, in the new draft guidance, *Basic* documentation is expected by default for the SaMD or SiMD, and a further assessment needs to be conducted to determine the need for *Enhanced* documentation. The draft guidance provides four risk-based criteria to aid in this assessment. Table 1, 2 and 3 provide side by side view of the buckets and type of documentation required subsequently.

Table 1: Risk Based Criteria and Documentation Decision Comparison

2005 Guidance (Level Of Concern)	**2021 Draft Guidance**
Major: If a failure or latent flaw could directly result in death or serious injury to the patient or operator. The level of concern is also Major if a failure or latent flaw could indirectly result in death or serious injury of the patient or operator through incorrect or delayed information or through the action of a care provider.	**Enhanced**: should be provided for any premarket submission that includes device software functions, where any of the following factors apply: 1. The device is a constituent part of a combination product 2. The device is (a) intended to test blood donations for transfusion-transmitted infections; or (b) used to determine donor and recipient compatibility; or (c) a Blood Establishment Computer Software. 3. The device is classified as class III. 4. A failure or latent flaw of the device software function(s) could present a probable risk of death or serious, either to a patient, user of the device, or others in the environment of use. These risk(s) should be assessed prior to implementation of risk control measures. You should consider the risk(s) in the context of the device's intended use; the direct and indirect impacts to safety, treatment, and/or diagnosis; and other relevant considerations.
Moderate: If a failure or latent design flaw could directly result in minor injury to the patient or operator. The level of concern is also Moderate if a failure or latent flaw could indirectly result in minor injury to the patient or operator through	**Basic**: Basic Documentation should be provided for any premarket submission that includes device software functions where Enhanced Documentation does not apply.

2005 Guidance (Level Of Concern)	2021 Draft Guidance
incorrect or delayed information or through the action of a care provider.	
Minor: If failures or latent design flaws are unlikely to cause any injury to the patient or operator.	

Table 2: Comparison between 2005-Guidance Minor/Moderate with 2021-Draft Basic

Documentation Level	Minor (2005 Guidance)	Moderate (2005 Guidance)	Basic (2021 Draft Guidance)
Documentation Level Evaluation (2005 Guidance called this Level of Concern)	A statement indicating the Level of Concern and a description of the rationale for that level.		A statement indicating the appropriate Documentation Level and a description of the rationale for that level.
Software Description	A summary overview of the features and software operating environment.		Software description, including overview of operationally significant software features, analyses, inputs, and outputs.
System and Software Architecture Design Chart	None	Detailed depiction of functional units and software modules. May include state diagrams as well as flow charts.	Detailed diagrams of the modules, layers, and interfaces that comprise the device, their relationships, the data inputs/outputs and flow of data, and how users or external products (including IT infrastructure and peripherals) interact with the system and software.
Risk Management File (2005 Guidance – Device Hazard Analysis)	Tabular description of identified hardware and software hazards, including severity assessment and mitigations.		Risk management plan, risk assessment demonstrating that risks have been appropriately mitigated, and risk management report.
Software Requirements Specification	Summary of functional requirements from SRS.	The complete SRS document.	The complete documentation, describing the needs or expectations for a system or software, presented in an organized format and with sufficient information to understand the traceability of the information with respect to the other software documentation elements (e.g., risk management file,

Documentation Level	Minor (2005 Guidance)	Moderate (2005 Guidance)	Basic (2021 Draft Guidance)
			software design specification, system and software architecture design chart, software testing as part of verification and validation).
Software Design Specification	None	Software design specification document.	None.
Software Development and Maintenance Practices	None	Summary of software lifecycle development plan including a summary of the configuration management and maintenance activities.	A Declaration of Conformity to IEC 62304 OR a summary of the life cycle development plan and a summary of configuration management and maintenance activities
Traceability Analysis	Traceability among requirements, specifications, identified hazards and mitigations, and Verification and Validation testing.		Included as part of Software Requirements Specification.
Software Testing as Part of Verification and Validation	Software functional test plan, pass/fail criteria, and results.	Description of V&V activities at the unit, integration, and system level. System level test protocol, including pass/fail criteria, and tests results.	A summary description of the testing activities at the unit, integration and system levels. System level test protocol including expected results, observed results, pass/fail determination, and system level test report.
Revision Level History	Revision history log, including release version number and date.		Revision history tabulating the major changes to the software during the development cycle, including date, version number, a brief description of the changes relative to the previous version, and indication of the version on which testing was performed.
Unresolved Anomalies (e.g., Bugs, Defects, or Errors)	None.	List of remaining software anomalies, annotated with an explanation of the impact on safety or effectiveness, including operator	List of remaining software anomalies (e.g., bugs, defects) annotated with an explanation of the impact on safety or effectiveness, including operator usage and human factors, workarounds, and timeframe for correction.

Documentation Level	Minor (2005 Guidance)	Moderate (2005 Guidance)	Basic (2021 Draft Guidance)
		usage and human factors.	

Table 3: Comparison between 2005 Guidance-Major with 2021 Draft-Enhanced

Documentation Level	*Major* (2005 Guidance)	*Enhanced* (2021 Draft Guidance)
Documentation Level Evaluation (2005 Guidance called this Level of Concern)	A statement indicating the Level of Concern and a description of the rationale for that level.	A statement indicating the appropriate Documentation Level and a description of the rationale for that level.
Software Description	A summary overview of the features and software operating environment.	Software description, including overview of operationally significant software features, analyses, inputs, and outputs.
System and Software Architecture Design Chart	Detailed depiction of functional units and software modules. May include state diagrams as well as flow charts.	Detailed diagrams of the modules, layers, and interfaces that comprise the device, their relationships, the data inputs/outputs and flow of data, and how users or external products (including IT infrastructure and peripherals) interact with the system and software.
Risk Management File (2005 Guidance – Device Hazard Analysis)	Tabular description of identified hardware and software hazards, including severity assessment and mitigations.	Risk management plan, risk assessment demonstrating that risks have been appropriately mitigated, and risk management report.
Software Requirements Specification	The complete SRS document.	The complete documentation, describing the needs or expectations for a system or software, presented in an organized format and with sufficient information to understand the traceability of the information with respect to the other software documentation elements (e.g., risk management file, software design specification, system and software architecture design chart, software testing as part of verification and validation).
Software Design Specification	Software design specification document.	The complete documentation, including sufficient information

Documentation Level	*Major* (2005 Guidance)	*Enhanced* (2021 Draft Guidance)
		that would allow FDA to understand the technical design details of how the software functions, how the software design completely and correctly implements all the requirements of the SRS and how the software design traces to the SRS in terms of intended use, functionality, safety, and effectiveness.
Software Development and Maintenance Practices	Summary of software life cycle development plan. Annotated list of control documents generated during development process. Include the configuration management and maintenance plan documents.	A Declaration of Conformity to IEC 62304 OR Basic Documentation Level PLUS complete configuration management and maintenance plan document(s)
Traceability Analysis	Traceability among requirements, specifications, identified hazards and mitigations, and Verification and Validation testing.	Included as part of Software Requirements Specification.
Software Testing as Part of Verification and Validation	Description of V&V activities at the unit, integration, and system level. Unit, integration and system level test protocol, including pass/fail criteria, test report, summary, and test results.	Basic Documentation Level PLUS unit and integration level test protocols including expected results, observed results, pass/fail determination, and unit and integration level test reports.
Revision Level History	Revision history log, including release version number and date.	Revision history tabulating the major changes to the software during the development cycle, including date, version number, a brief description of the changes relative to the previous version, and indication of the version on which testing was performed
Unresolved Anomalies (e.g., Bugs, Defects, or Errors)	List of remaining software anomalies, annotated with an explanation of the impact on safety or effectiveness, including operator usage and human factors.	List of remaining software anomalies (e.g., bugs, defects) annotated with an explanation of the impact on safety or effectiveness, including operator usage and human factors, work-

Documentation Level	*Major* (2005 Guidance)	*Enhanced* (2021 Draft Guidance)
		arounds, and timeframe for correction

Essentially, the new draft guidance eliminates the *Minor* level of concern, and requires much *more* information to be submitted at the *Moderate* level of concern with the exception of Software Requirements Document, and Software Design Document. The documentation is comparable in some cases between *Major* level of concern and the *Enhanced* category with many more details in other cases.

Following are the key take-aways for further assessments by organizations:

1. Stand Alone Software Risk Management for SaMD or Software Risk as part of the Device Risk Management. Note that, documentation will include a lot more than just the risk assessment.
2. Off the Shelf Software documentation
3. Cybersecurity and Risk Management
4. Traceability expands to all levels of software documentation and risk management file
5. Application of "probable" term in determining the risk
6. Software Unresolved Anomalies and categorization per ANSI/AAMI SW91.
7. The specific use of IEC 62304 considering the similarities (process focused elements) and differences (actual deliverables) between the intents and information covered in the new draft guidance and IEC 62304.

In conclusion, the new guidance would require organizations to perform a high-level assessment in order to put a proactive response plan in place. These incipient changes may require updates to procedures and may impact product development timelines. The latter is true especially for products where the existing plan call for submitting the software at a *Minor* Level of Concern.

About Triple Ring Technologies

Triple Ring Technologies is a co-development company headquartered in Silicon Valley, with offices in Boston, Toronto, and Copenhagen. They partner with clients in medtech, life sciences, and sustainability & the environment to create new technologies, launch innovative projects, and start new ventures. Their capabilities span early R&D, product development, manufacturing, regulatory approval, market access, strategic investment, and incubation. For more information, please visit www.tripleringtech.com.