**Software/Firmware & Cybersecurity/Interoperability**

**1 Software**

* 1. Software Level of Concern (LOC) Determination

*【Please use our Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices to ensure you have properly documented and tested your device. The software guidance applies to devices that contain one or more software components, parts, or accessories, or are composed solely of software as “software devices,” including:*

* *Firmware and other means for software-based control of medical devices*
* *Stand-alone software applications*
* *Software intended for installation in general-purpose computers*
* *Dedicated hardware/software medical devices*
* *Accessories to medical devices when those accessories contain or are composed of software*

*The software guidance applies to software devices regardless of the means by which the software is delivered to the end user, whether factory-installed, installed by a third-party vendor, or field-installed or -upgraded.*

*Resources:*

*Guidance: “Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices”*

*Guidance: “General Principles of Software Validation; Final Guidance for Industry and FDA Staff”*

*Guidance: “Off-The-Shelf Software Use in Medical Devices”】*

* + 1. Does the Software qualify as Blood Establishment Computer Software?

*【Blood Establishment Computer Software is defined as software products intended for use in the manufacture of blood and blood components or for the maintenance of data that blood establishment personnel use in making decisions regarding the suitability of donors and the release of blood or blood components for transfusion or further manufacture.】*

* + 1. Is the Software intended to be used in combination with a drug or biologic?
    2. Is the Software an accessory to a medical device that has a Major LOC?
    3. Prior to mitigation of hazards, could a failure of the Software result in death or serious injury, either to a patient or to a user of the device?
    4. Is the Software an accessory to a medical device that has a Moderate LOC?
    5. Prior to mitigation of hazards, could a failure of the Software result in Minor Injury, either to a patient or to a user of the device?
    6. Could malfunction of, or a latent design flaw in, the software lead to an erroneous diagnosis or a delay in delivery of appropriate medical care that would likely lead to Minor Injury?
    7. Based on the questions answered above, your LOC is determined to be:
  1. Software Description

*【Specify the name of the software*

*Specify the version of the software - The version tested should be clearly identified and should match the release version of the software, otherwise justification must be provided.*

*Provide a description of the software including the identification of the device features that are controlled by the software, the programming language, hardware platform, operating system (if applicable), use of Off-the-shelf software (if applicable), a description of the realization process.*

*Provide a statement about software version naming rules, specify all fields and their meanings of software version, and determine the complete version of software and its identification version used for release.】*

1.3 Software Documentation

1.3.1 Device Hazard Analysis

*【The Device Hazard Analysis should take into account all device hazards associated with the device’s intended use, including both hardware and software hazards. This document can be in the form of an extract of the software-related items from a comprehensive risk management document, such as the Risk Management Summary described in ISO 14971, In this format, each line item should include:*

* *Identification of the hazardous event*
* *Severity of the hazard*
* *Cause(s) of the hazard*
* *Method of control (e.g., alarm, hardware design)*
* *Corrective measures taken, including an explanation of the aspects of the device design/requirements, that eliminte, reduce, or warn of a hazardous event; and*
* *Verification that the method of control was implemented correctly.*

*】*

1.3.2 Software Requirements Specifications (SRS)

*【The software Requirements Specifications (SRS) documents the requirements for the software. This typically includes functional, performance, interface, design, developmental, and other requirements for the software. In effect, this document describes what the software device is supposed to do.*

*Minor LOC:*

*Documentation should include a summary functional requirements section from the SRS, including identification of off-the-shelf software.*

*Major to Moderate LOC:*

*The complete SRS should be included.】*

1.3.3 Architecture Design Chart

*【The Architecture Design Chart is typically a flowchart of similar depiction of the relationships among the major functional units in the Software Device, including relationships to hardware and to data flows such as networking. It is usually not necessary to include every function call and module in this document; however, there should be sufficient information to allow for review of the organization of the software relative to the functionality and to the intended use of the Software Device. If the Architecture Design Chart is included in another document such as the SRS, a reference to the location of the Architecture Design Chart in the submission should be included.】*

1.3.4 Software Design Specifications (SDS)

*【The software Design Specification (SDS) describes the implementation of the requirements for the Software Device. In terms of the relationship between the SRS and the SDS, the SRS describes what the Software Device will do and the SDS describes how the requirements in the SRS are implemented. The information presented in the SDS should be sufficient to ensure that the work performed by the software engineers who created the Software Device was clear and unambiguous, with minimal ad-hoc design decisions. The SDS may contain references to other documents, such as detailed software specifications. However, the document should, in and of itself, provide adequate information to allow for review of the implementation plan for the software requirements in terms of intended use, functionality, safety, and effectiveness.】*

1.3.5 Traceability Analysis/Matrix

*【A Traceability Analysis links together the product design requirements, design specifications, and testing requirements. It also provides a means of tying together identified hazards with the implementation and testing of the mitigations. The traceability among these activities and associated documentation should be explicit because they are essential to effective product development and to our understanding of product design, development and testing, and hazard mitigations. The Traceability Analysis commonly consists of a matrix with line items for requirements, specifications and tests, and pointers to hazard mitigations. It is possible to document traceability simply through a shared organizational structure with a common numbering scheme; however, it should include some mechanism, such a matrix for guiding the reviewer through the submitted information.】*

1.3.6 Software Development Environment/Life Cycle Process Description

*【The software Development Environment/Life Cycle Process Description should describe the software development life cycle and the processes that are in place to manage the various life cycle activities.*

*Moderate LOC:*

*Documentation should include a summary of the configuration management and maintenance plans.*

*Major LOC:*

*Documentation should include an annotated list of the control/baseline documents generated during the software development process and a list or description of software coding standards. Changes to the Software Devices after initial market release should be subject to positive control, with definitive specification and test plans including well-defined regression testing where appropriate. The description of the development environment should provide information on the configuration management and maintenance plan that addresses these aspects of the software development life cycle. Sufficient detail should be provided to allow for a thorough understanding of the configuration management and maintenance plan.】*

1.3.7 Verification & Validation Testing

*【The following should be included in your Verification and Validation Testing for your Level of Concern.*

*Minor LOC:*

*This should include a software functional test plan, pass/fail criteria, and results.*

*Moderate LOC:*

*This should include a description of V&V activities at the unit, integration, and system level. It should also include system level test protocol, including pass/fail criteria, and tests results.*

*Major LOC:*

*This should include a description of V&V activities at the unit, integration, and system level. This should also include unit, integration and system level test protocols, including pass/fail criteria, test report, summary, and test results.*

*Although software verification may be performed using a per function test protocol, validation (e.g., actual user testing of the device’s user interface including input and output testing of the program structure) should be done on the completed software. Although the verification ensures that the device performs as designed, the validation is needed to test these designs and ensure they are appropriate for the environments they will be used in (i.e., appropriate for the users and applications for which they are designed).】*

1.3.8 Revision Level History

*【The Revision Level History should include the history of software revisions generated during the course of product development. This typically takes the form of a line-item tabulation of the major changes to the software during the development cycle, including date, version. The last entry in the list should be the final version to be incorporated in the released device. This entry should also include any differences between the tested version of software and the released version, along with an assessment of the potential effect of the differences on the safety and effectiveness of the device.】*

1.3.9 Unresolved Anomalies

*【Unresolved Anomalies documentation should include a list of remaining software anomalies, annotated with an explanation of the impact on safety or effectiveness, including operator usage and human factors. The description of each anomaly should include the:*

* *Problem*
* *Impact on device performance*
* *Any plans or timeframes for correcting the problem (where appropriate).】*

**2 Cybersecurity**

*【Please use our guidance entitled “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices,” “Postmarket Management of Cybersecurity in Medical Devices,” as well as “Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices,” to ensure you have properly documented and tested the device.*

*Only provide documentation regarding cybersecurity and Interoperability if the device/system fulfills any of the following criteria:*

* *Can communicate with other devices/systems,*
* *Has a network/server connection or potential for a future network/server connection that should be disabled,*
* *Has the potential for unused ports for network connections,\*
* *Uses any form of wireless communication (e.g. Bluetooth, Wi-Fi, cellular, RF, inductive),*
* *Has a USB port/physical media access (e.g. memory card, JTAG),*
* *Allows for software/firmware downloads (e.g. software/firmware updates or patching),*
* *Allows for cloud storage or cloud services.*

*Providing documentation regarding the Cybersecurity is required if the submission is a 510(k), PMA, De Novo, or HDE, and any of the above conditions are met.*

*Providing documentation regarding the Interoperability of your device is recommended if the submission is a Traditional or Abbreviated 510(k), and any of the above conditions are met. If the submission is a Special 510(k), and any of the above conditions are met, documentation is only recommended if any changes to the device(in comparison to the primary predicate) could affect the Interoperability of the device.*

*Resources*

*Guidance:“Content of Premarket Submissions for Management of Cybersecurity in Medical Devices”*

*Guidance: “Design Considerations and Premarket Submission Recommendations for Interoperable Medical Devices”*

*Guidance: “Postmarket Management of Cybersecurity in Medical Devices ”】*

2.1 Risk Management

*【Manufacturers are required to provide certain information in their premarket submissions per Section 524B of the FD&C Act. The 2014 Premarket Cybersecurity Guidance discusses the following activities as part of the validation and risk analysis for cybersecurity (Section 4), which may be helpful in providing the required information:*

* *Identification of assets, threats, and vulnerabilities;*
* *Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients;*
* *Assessment of the likelihood of a threat and a vulnerability being exploited;*
* *Determination of risk levels and suitable mitigation strategies;*
* *Assessment of residual risk and risk acceptance criteria.*

*Risk management for cybersecurity includes an assessment of the system to understand the parts of the device that are vulnerable to a cybersecurity attack (often referred as “the attack surface” in cybersecurity literature) along with the assessment of the assets, vulnerabilities, and risk controls employed. The compilation of the assets, vulnerabilities, and risk controls are collectively called the threat model.*

*The concepts (Identify, Protect, Detect, Respond, and Recover) in Section 5 of the 2014 Premarket Cybersecurity Guidance should be incorporated into the risk management documentation.*

*The concepts (Vulnerabilities/Risks, Controls, Traceability Matrix, Malware-Free Shipping) in Section 6 of the Premarket Cybersecurity Guidance should be incorporated into the risk management.*

*Resources*

*Threat Modeling:*

*Threat Modeling documentation should address cybersecurity during the design and development of the medical device and related systems, as this can result in more robust and efficient mitigation of patient risks. Section 4 of the 2014 Premarket Cybersecurity Guidance, Section 6, Item 1). The threat model should consider that threats change as new vulnerabilities are discovered and ways to exploit them are published (these are known as threat actors), which is one of the elements which distinguishes threat modeling from traditional risk assessment.*

*Cybersecurity Risk Assessment:*

*The 2014 Premarket Cybersecurity Guidance discusses the following risk assessment activities for cybersecurity (Section 4):*

* *Identification of assets, threats, and vulnerabilities;*
* *Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients;*
* *Assessment of the likelihood of a threat and of a vulnerability being exploited;*
* *Determination of risk levels and suitable mitigation strategies;*
* *Assessment of residual risk and risk acceptance criteria.*

*These assessments can be documented in a cybersecurity risk assessment. The Postmarket Cybersecurity Guidance recommends that manufacturers use exploitability to assess the likelihood of cybersecurity risks. This assessment should analyze the assets, threats, vulnerabilities, and controls identified in the threat modeling to determine any impact to the device performance and impact to the environment as well as patient safety. (2014 Premarket Cybersecurity Guidance, Section 6, Item 1).*

*Unresolved Anomalies:*

*Unresolved anomalies are discussed in the FDA Guidance “Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices.” Software anomalies can cause security risks for the device which may impact the safety and effectiveness.*

*Cybersecurity Controls*

*Section 5 of the 2014 Premarket Cybersecurity Guidance recommends that manufacturers provide justifications for the security functions chosen for their medical device. These cybersecurity functions include but may not be limited to:*

* *Limit Access to Trusted Users Only*
  + *Limit access to devices through the authentication of users (e.g. user ID and password, smartcard, biometric)*
  + *Use automatic timed methods to terminate sessions within the system where appropriate for the use environment*
  + *Where appropriate, employ a layered authorization model by differentiating privileges based on the user role (e.g. caregiver, system administrator) or device role*
  + *Use appropriate authentication (e.g. multi-factor authentication to permit privileged device access to system administrators, service technicians, maintenance personnel)*
  + *Strengthen password protection by avoiding “hardcoded” password or common words (i.e. passwords which are the same for each device, difficult to change, and vulnerable to public disclosure) and limit public access to passwords used for privileged device access*
  + *Where appropriate, provide physical locks on devices and their communication ports to minimize tampering*
  + *Require user authentication or other appropriate controls before permitting software or firmware updates, including those affecting the operating system, applications, and anti-malware.*
* *Ensure Trusted Content*
  + *Restrict software or firmware updates to authenticated code. One authentication method manufacturers may consider is code signature verification*
  + *Use systematic procedures for authorized users to download version-identifiable software and firmware from the manufacturer*
  + *Ensure capability of secure data transfer to and from the device, and when appropriate, use methods for encryption.*
* *Detect, Respond, Recover*
* *Implement features that allow for security compromises to be detected, recognized, logged, timed, and acted upon during normal use*
* *Develop and provide information to the end user concerning appropriate actions to take upon detection of a cybersecurity event*
* *Implement device features that protect critical functionality, even when the device’s cybersecurity has been compromised*
* *Provide methods for retention and recovery of device configuration by an authenticated privileged user.】*

Traceability Matrix

A traceability matrix links actual cybersecurity controls to the cybersecurity vulnerabilities/risks that were considered (2014 Premarket Cybersecurity Guidance, Section 6, Item 2). This matrix may also include traceability to the cybersecurity testing performed to evaluate the controls.

Cybersecurity Testing

FDA has recognized the consensus standards: AAMI/UL 2900-1:2017 and IEC 810001-5-1:2021 which may be helpful to support cybersecurity documentation in submissions. These standards both include cybersecurity testing as a part of the device design and evaluation activities. See AAMI/UL 2900-1:2017, Clause 13-19 or IEC 81001-51:2021, Clause 5.5-5.7 for cybersecurity testing types that may support demonstrating that the cybersecurity controls and requirements are effective.

SBOM and Supporting Info

Section 524B(b)(3) of the FD&C requires that you provide a software bill of materials (SBOM) for the commercial, open-source, and off-the-shelf software components. There are resources available to assist in understanding SBOMs including the minimum elements (also referred as “baseline attributes”) identified in the October 2021 National Telecommunications and Information Administration (NTIA) Multistakeholder Process on Software Component Transparency document “Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM).”

Additionally, Section V. of the FDA Guidance “Off-The-Shelf Software Use in Meical Devices” identifies document recommendations including a harzard analysis for OTS software. Vulnerabilities in the OTS software can present hazards and may be assessed in such documentation or provided with the SBOM information.

2.2 Cybersecurity Management Plan / Plan for Continuing Support

*【Section 524B(b)(1) of the FD&C Act requires that you provide a plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures.*

*Section 524B(b)(2) and 524(b)(2)(A) requires that you make available postmarket updates and patches to the device and related systems to address, on a reasonably justified regular cycle, known unacceptable vulnerabilities.*

*Section 524B(b)(2) and 524B(b)(2)(B) requires that you make available postmarket updates and patches to the device and related systems to address, as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks.*

*The 2014 Premarket Cybersecurity Guidance makes recommendations about managing the device postmarket and providing the plans as part of the premarket submission in Section 6, Items 3 and 4. Section X of the Postmarket Cybersecurity Guidance also makes recommendations about the elements of an effective postmarket cybersecurity program. The FDA typically will not need to review or approve medical device software chagnes made solely to strengthen cybersecurity as descrbied in teh Postmarket Cybersecurity Guidance.】*

2.3 Please specifically cite the attachment(s) and page number(s) where the cybersecurity labeling is located. (Note: If there is separate cybersecurity labeling for the device, please attach this in the Labeling section above.)

*【Cybersecurity Labeling includes device instructions for use and product specifications related to recommended cybersecurity controls appropriate for the intended use environment (e.g. antivirus software, use of firewall). This should be consistent with the risk controls described in the risk assessment as well as any configuration items necessary on the computer or computing platform (e.g., recommending popups be blocked). (2014 Premarket Cybersecurity Guidance, Section 6, Item 5).】*

**3 Interoperability**

3.1 How many Electronic Interfaces are there?

*【For purpose of this review, the electronic interface is the medium by which systems interact and/or communicate with each other thereby allowing the exchange of information between systems. It includes both the type of connection (e.g., USB port, wireless connection) and the information content. It is a medium by which a medical device exchanges and uses information with other requirement or other medical devices.】*

3.2 Electronic Interface 1

3.2.1 Name the Electronic Interface

3.2.2 Is the electronic interface inactive (i.e. not meant to connect, exchange, or use data with or from other medical devices, products, technologies, or systems)?

3.2.3 Are the interfaces only meant for service or maintenance?

3.2.4 Is the data flow only meant for transferring, storing, converting formats, or displaying clinical laboratory test and not intended to interpret or analyze clinical laboratory test or other device data, results, and findings?

3.2.5 Describe the Electronic Interface

*【You should include a discussion of each externally-facing electronic interface found on the device, the purpose of each interface, and the anticipated users of the interface. You should also describe how each interface is meant to be used and/or the limitations of the use of the interfafces. If the interface is only meant to be used by the manufacturer, this should be clearly stated. If the interface is meant to used with only specific devices, those devices should be clearly specified.*

*(Interoperability guidance, page 13)】*

3.2.6 Interoperability Risk Assessment / Verification and Validation

*【The risk analysis should address:*

*The risk control measures for reducing unacceptable risks to acceptable levels*

*Fault tolerant behavior, boundary conditions, and fail safe behavior such as how the device handles delays, corrupted data, and any other issues with the reception and transmission of data*

*Any risks potentially arising from security vulnerabilities that may be involved with the presence of an electronic interface*

*Risks arising from normal use as well as reasonably foreseeable misuse. For example, a manufacturer may want to include in the labeling an explicit warning against foreseeable uses that could result in harm.*

*The following performance testing should be included in the Verification and Validation documentation:*

*Verification that the device interface meets its design specifications*

*Validation that the device interface performs as intended*

*Determination and verification of the information that should be provided to a user to connect to the interface and allow the user to ensure that the connection has been made correctly*

*Verification that the device will perform safely and within specification when used under normal and abnormal conditions that are reasonably likely to occur (e.g. receives data outside of specification, connected to an unintended device or system, does not lock up the system when the interface is exercised)*

*The degree of documentation can vary based upon the risks associated with the device, the purpose of the interface, the anticipated use of the device in the interoperable system, and the intended use of the device. For interface elements that use a standard, demonstrating conformance to that standard may be sufficient.】*

3.2.7 Please specifically cite the attachment(s) and page number(s) where the interoperability labeling is located. (Note: If there is separate interoperability labeling for the device, please attach this in the Labeling section above.)

*【It is recommended that labeling include the following for the electronic interfaces (EI) as appropriate:*

* *Purpose of the EI (e.g., devices it is intended to connect to or control)*
* *Anticipated users*
* *Specifications for each EI (e.g., physiological waveforms, probe type, accuracy, frequency of response, update rate, data rate, bandwidth)*
* *Necessary performance and functional requirements*
* *List of data attributes exchanged*
* *Summary of EI testing to verify interoperability claims and activities suggested to verify safe operation (the representative device should be specified when testing was performed to an EI specification and verified with a representative device)*
* *Relevant standards and certifications*
* *Method for time synchronization*
* *Description of fault tolerance behavior, boundary condition testing or fail safe for critical functions*
* *Known limitations, contraindications, precautions and warnings*
* *Recommended connections, settings or configurations*
* *Specific user instructions 】*