Required Information to Support your 510(k) Submission

The list below provides a list of information (attachments, standalone documents, pictures or diagrams) required to support your submission.

This list is based on FDA's eStar Version 5.5 (2025-02-12) with the following assumptions:

- New application for a Traditional Premarket Notification 510(k)
- No previous pre-submission correspondence or previous regulatory submissions for this device
- Device is software only
- Device includes cloud communication, network connection (active or not), wireless communication, and software upgrades
- The following Electronic Interface exists: wireless communication for exchange of information/data between systems
- Bench testing will be used to support the submission
- Animal testing will **not** be used to support the submission
- Clinical testing will **not** be used to support the submission

Note that information on this list may change if the FDA eStar is updated between now and your submission date or if there are changes in the assumptions listed above.

File or item required to support your submission	Description
510(k) Cover Letter	Cover Letter for the submission. The cover letter should state the applicant or sponsor name and/or their authorized representative, the type of submission, the common name of the device, device trade name or proprietary name, and state the purpose of the application, including any changes being made to existing approvals. The cover letter should also include your preference for continued confidentiality (21 CFR 807.95).
List of applicable standards	Standards applicable to your device will need to be populated within the submission application.
Comprehensive Device Description and Principles of Operation	Should describe your device in detail. Include: 1) What the device does, 2) Who uses it and for what, 3) How it works, including a description of the features/variants/operating modes that enable the device to be used for indications/intended use (principle of operation/mechanism of action) and if not apparent for the device type, a brief description of the underlying science/technology, design concepts, and/or theoretical principles supporting the functions.

File or item required to support your submission	Description
	Note that the detailed device description can be included within another document, such as your User Needs.
Device Pictures, Illustrations, Schematics, Diagrams OR Justification for no physical form	For the software-only device, include a justification if the device does not have a physical form.
Substantial Equivalence Discussion	Include an analysis of why any differences between the subject device and predicate(s) do not affect safety or effectiveness, or raise different types of questions of safety and effectiveness.
Package Labeling OR Justification for no package labeling	For the software-only device, include a justification for why this documentation is not applicable.
Package Insert / Instructions for Use	Included copies of the User Instructions, Inserts, Directions for Use and/or Instructions for Use that are intended for use with your device. This includes instructions that may be downloaded or viewed on a website.
Documentation Level Evaluation	A statement should be provided indicating the Documentation Level for the device and a description of the rationale for such Documentation Level. The rationale should account for the device's intended use, and include references, where appropriate, from the submission documentation (such as Risk Management File, Software / Firmware Description, etc.) to support the indicated Documentation Level. *(see Section V. of the FDA Guidance Content of Premarket Submissions for Device SW Functions https://www.fda.gov/media/153781/download)*
Software Description (to be included in your SDS)	The software description should include: 1. a comprehensive overview of significant software features and functions, which may include images, flow charts, and state diagrams as needed to adequately explain the software functionality, 2. specification of the version of the software - The version tested must be clearly identified and should match the release version of the software, otherwise justification must be provided, and 3. 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

File or item required to support your submission	Description
	of the realization process. For your AI algorithms, include the following information for each: ● a detailed description of each algorithm/model, including its inputs, outputs, data selection and management for training, testing, and validation (terminology may differ in different regions); ● High-level architecture showing all of the logic units followed by a description of each including each units inputs, outputs, and what processing/function it provides. ● Comprehensive training methodology description ● model selection and evaluation; ● materials/approaches used to provide transparency; and A description of the off-the-shelf (OTS) software (if applicable) should also be included. This software description can be included in your Software Design Specification (see below). *(see Section VI. B of the FDA Guidance Content of Premarket Submissions for Device SW Functions https://www.fda.gov/media/153781/download)*
Risk Management File	The following documents are part of this file and include these separate documents: ● Risk management plan, ● Risk assessment (hazard analysis), and ● Risk management report. *(See ISO 14971 and see Section VI. C of the FDA Guidance Content of Premarket Submissions for Device SW Functions https://www.fda.gov/media/153781/download)*
Software Requirements Specification (SRS)	The SRS documentation should describe the needs or expectations for a system or software, presented in an organized format, at the software system level or subsystem level, as appropriate, and with sufficient information to understand the traceability of the information with respect to the other software documentation elements. The SRS documents the requirements for the software which typically

File or item required to support your submission	Description
	specifies inputs and outputs, functions that the software will perform, hardware, performance, interfaces, user interaction, error definition and handling, intended operating environment, safety related requirements derived from a risk assessment (hazard analysis) and all ranges, limits, defaults, and specific values that the software will accept. *(see Section VI. D of the FDA Guidance Content of Premarket Submissions for Device SW Functions https://www.fda.gov/media/153781/download)*
System & Software Architecture Design (SAD) Chart (can be included in your SDS)	Should consist of 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. Note that this information can be included within another document, such as the SRS. If the SAD Chart is included in another document, a reference to the location of the SAD Chart in the submission should be included. *(see Section VI. E of the FDA Guidance Content of Premarket Submissions for Device SW Functions https://www.fda.gov/media/153781/download)*
Software Design Specifications (SDS)	Should include sufficient information 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. In terms of the relationship between the SRS and the SDS, the SRS describes what the software function 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 device software function was clear and unambiguous, with minimal ad hoc design decisions. *(see Section VI. F of the FDA Guidance Content of Premarket Submissions for Device SW Functions https://www.fda.gov/media/153781/download)*
Software Lifecycle Process Description / Software Development,	Should describe the software development life cycle and the processes that are in place to manage the various life cycle activities. Note that this information can be included within another document, such as

File or item required to support your submission	Description
Configuration Management, and Maintenance Practices	the SRS or Software Architecture document. *(see Section VI. G of the FDA Guidance Content of Premarket Submissions for Device SW Functions https://www.fda.gov/media/153781/download)*
Software Testing as part of V&V	Should provide an overall description of the verification and validation activities performed for the final software version. Should provide the applicable test protocols and reports including the expected results, observed results and pass/fail determination. **Basic Documentation Level:** A summary description of the testing activities at the unit, integration and system levels; AND system level test protocol including expected results, observed results, pass/fail determination, and system level test report. **Enhanced Documentation Level:** 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. *(see Section VI. H of the FDA Guidance Content of Premarket Submissions for Device SW Functions https://www.fda.gov/media/153781/download)*
Software Version / Revision Level History	Should include the history of software versions that were tested and documented at the unit, integration, and system levels as part of verification and validation activities. This document typically takes the form of a line-item tabulation including the date, version number that was tested and a brief description of all changes in the version relative to the previously tested version. The last entry in a line-item tabulation 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. *(see Section VI. I of the FDA Guidance Content of Premarket Submissions for Device SW Functions https://www.fda.gov/media/153781/download)*
Software Unresolved Anomalies	Should include a list of unresolved anomalies present in the software with the following items for each unresolved anomaly:

File or item required to support your submission	Description
	• A description of what the anomaly is and what the root cause(s) of the anomaly could be; • Identification of how the anomaly was discovered and, where possible, identification of the root cause(s) of the anomaly; • Evaluation of the impact of the anomaly on the device's safety and effectiveness, including operator usage and human factors considerations; • Outcome of the evaluation; and • Risk-based rationale for not correcting or fixing the anomaly in alignment with the risk management plan or procedures. *(see Section VI. J of the FDA Guidance Content of Premarket Submissions for Device SW Functions https://www.fda.gov/media/153781/download)*
Cybersecurity Risk Management Report	Should include the following items: • Risk analysis, mitigations, and design considerations pertaining to cybersecurity risks, • A traceability matrix of security risks to security controls, • Traceability to the verification reports for documented security controls, • A description of when and how security updates/patches will be provided, • A description of the steps taken to assure devices will be delivered malware-free. In addition, this security risk management report should: • Summarize the risk evaluation methods and processes, • Detail the residual risk conclusion from the security risk assessment, • Detail the risk mitigation activities undertaken as part of a manufacturer's risk management processes, • Provide traceability between the threat model, cybersecurity risk assessment, SBOM, and testing documentation as well as other relevant cybersecurity risk management documentation. *(see Section V. A of the FDA Cybersecurity Guidance https://www.fda.gov/media/119933/download)*
Threat Model Documentation	Should include threat modeling for the entire medical device system including all end-to-end connections into and/or out of the system. The Threat Model documentation should:

File or item required to support your submission	Description
	• Identify medical device system risks and mitigations as well as inform the pre- and post-mitigation risks considered as part of the cybersecurity risk assessment, • State any assumptions about the medical device system or environment of use, • Capture cybersecurity risks introduced through the supply chain, manufacturing, deployment, interoperation with other devices, maintenance/update activities, and decommission activities that might otherwise be overlooked in a traditional safety risk assessment process. A rationale for the threat methodology(ies) selected should be provided with the threat modeling documentation. *(see Section V.A.1 of the FDA Cybersecurity Guidance https://www.fda.gov/media/119933/download)*
Cybersecurity Risk Assessment	Should be a separate risk assessment from the safety risk management process and capture the risks and controls identified from the threat model. Identified risks should be assessed according to the level of risk posed from the device and the system in which it operates. Acceptance criteria for cybersecurity risks should carefully consider the total product lifecycle of the medical device system. The methods used for scoring the risk pre- and post-mitigation and the associated acceptance criteria as well as the method for transferring security risks into the safety risk assessment process should be provided. Security risks and controls should be assessed for residual risks and address the fact that cybersecurity-related failures can occur either intentionally or unintentionally. *(see Section V.A.2 of the FDA Cybersecurity Guidance https://www.fda.gov/media/119933/download)*
Software Bill of Materials (SBOM)	Should include both the device manufacturer-developed components and third-party components, including purchased/licensed software and open-source software, and the upstream software dependencies that are required/depended upon by proprietary, purchased/licensed, and open-source software. Provide a machine-readable SBOM consistent with the minimum elements (baseline attributes) identified in the September 2024 Cybersecurity and

File or item required to support your submission	Description
	Infrastructure Security Agency (CISA) document “Framing Software Component Transparency: Establishing a Common SBOM, Third Edition” https://www.cisa.gov/sites/default/files/2024-10/SBOM%20Framing%20Software%20Component%20Transparency%202024.pdf
Software Level of Support and End-of-Support dates for SBOM components	This document should provide the software level of support and end-of support date for each software component identified in the SBOM. For any component where this information was not available, provide a Justification. You may choose to provide these additional elements as part of the SBOM, or they may provide it separately, such as in an addendum.
Vulnerabilities Assessment	Should identify all known vulnerabilities associated with the device and the software components, including those identified in CISA’s Known Exploited Vulnerabilities Catalog (www.cisa.gov/known-exploited-vulnerabilities-catalog) and the NIST National Vulnerability Database (nvd.nist.gov/vuln). For each known vulnerability, manufacturers should describe how the vulnerability was discovered to demonstrate whether the assessment methods were sufficiently robust. For components with known vulnerabilities, you should provide: ● 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 compensating controls should be described in an appropriate level of detail.
Unresolved Cybersecurity Anomalies	Provide an assessment of any unresolved anomalies for cybersecurity impact. If none exist, attach a document stating that no unresolved anomalies exist.
Cybersecurity Metrics Data	Provide data from monitoring cybersecurity metrics. Manufacturers should provide the following measures and metrics: ● 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

File or item required to support your submission	Description
	implementation in devices deployed in the field, to the extent known. If metric data are unavailable, a justification should be provided.
Cybersecurity Controls	Provide information on the security controls categories included as part of the device. Cybersecurity controls should address the following: ● Authentication ● Authorization ● Cryptography ● Code, data, and execution integrity ● Confidentiality ● Event detection and logging ● Resiliency and recovery ● Firmware and software updates *(see Section V.B.1 of the FDA Cybersecurity Guidance https://www.fda.gov/media/119933/download)*
Architecture Views Documentation	Should include architecture views of the following: Global System View, Multi-Patient Harm View, Updatability/Patchability View, and Security Use Case Views. These views should include both diagrams and explanatory text. These diagrams and explanatory text should contain sufficient details to permit an understanding of how the assets within the medical device system function holistically within the associated implementation details. Note that these Architecture Views can be included within another document, such as the Threat Modeling documentation or SW Architecture document. *(see Section V.B.2 of the FDA Cybersecurity Guidance https://www.fda.gov/media/119933/download)*
Cybersecurity Testing Documentation	Should describe the cybersecurity testing performed and the associated test reports. Cybersecurity testing includes but may not be limited to security requirement testing, threat mitigation testing, vulnerability testing, and penetration testing. If security testing was performed by a third party, provide the original third party test report and your assessment of any findings. Alternatively, provide a justification for why particular testing was not performed. *(see Section V.C of the FDA Cybersecurity Guidance https://www.fda.gov/media/119933/download)*
Cybersecurity	This plan should detail how you will identify and communicate to users

File or item required to support your submission	Description
Management Plan	vulnerabilities that are identified after releasing the device. The plan should detail how to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures. *(see Section VI.B of the FDA Cybersecurity Guidance https://www.fda.gov/media/119933/download)*
Bench Testing Documentation	Should attach documentation that includes details of nonclinical bench testing performed with your device (test report, characterization, etc). This should include information about any tests/studies/evidence conducted to support your submission. Full test reports should include: objective of the test, description of the test methods and procedures, study endpoint(s), pre- defined pass/fail criteria, results summary, conclusions, and an explanation of how the data generated from the test supports your submission. *(see FDA Guidance "Recommended Content and Format of Non-Clinical Bench Performance Testing Information in Premarket Submissions"https://www.fda.gov/media/113230/download)*
OTHER DICOM Conformance Statement	While the 510(k) eStar file does not have a specific section for this, a DICOM conformance statement for your subject device should also be attached to your submission file. This document should detail the exact features of the DICOM standard supported by your device. It should support the interoperability between your device and other systems intended to integrate with your device. *(see FDA Guidance "Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices" https://www.fda.gov/media/95636/download)*
OTHER Coordinated Vulnerability Disclosure	While the 510(k) eStar file does not have a specific section for this, a description of your coordinated vulnerability disclosure (CVD) process should be attached. The CVD should address the manufacturer's formalized processes for the following: ● obtaining cybersecurity vulnerability information,

File or item required to support your submission	Description
	● assessing vulnerabilities, ● developing remediation strategies, and ● how to disclose the existence of vulnerabilities and remediation approaches to its various stakeholders. Note that this could be a standalone document, or included as part of your Cybersecurity Management Plan.
OPTIONAL General Summary of Submission / Executive Summary	A general summary can be attached to the Administrative Section of your 510(k) submission eStar file. This summary should include a concise description of the device, including the indications for use and technology, a concise summary for any performance testing in the submission, and a comparison to the predicate device(s).