Table of Contents

1. PURPOSE

The purpose of this document is to describe how safety and security risks in CT Cardiomegaly are managed.

2. SCOPE

This plan applies to CT Cardiomegaly across all phases of the product development lifecycle.

3. DEFINITIONS

Terms and abbreviations used within this document:

Term	Definition
Problem Report	A record of actual or potential behaviour of the software that a user or other interested person believes to be unsafe, inappropriate for the intended use or contrary to specification.
Requirement	A statement about something the design must accomplish. Good requirements are verifiable, necessary, irreducible, and don't prescribe a design.
Risk Analysis	systematic use of available information to identify hazards and to estimate the risk.
Risk Control	Process in which decisions are made and measures implemented by which risks are reduced to, or maintained within, specified levels.
Risk Management	Systematic application of management policies, procedures (3.13) and practices to the tasks of analyzing, evaluating, controlling and monitoring risk
SBOM	Software Bill Of Materials
Serious Injury	From the QSR, an injury or illness that: (1) Is life-threatening, (2) Results in permanent impairment of a body function or permanent damage to a body structure, or (3) Necessitates medical or surgical intervention to preclude permanent impairment of a body function or permanent damage to a body structure.

Term	Definition
	Permanent means irreversible impairment or damage to a body structure or function, excluding trivial impairment or damage.
System	Integrated composite consisting of one or more of the processes, hardware, software, facilities, and people that provides a capability to satisfy a stated need or objective.
UI	User Interface
User	Person who interacts with (i.e., operates or handles) the device.
User Interface	All points of interaction between the user and the device, including all elements of the device with which the user interacts (i.e., those parts of the device that users see, hear, touch). A ll sources of information transmitted by the device (including packaging, labeling), training and all physical controls and display elements (including alarms and the logic of operation of each device component and of the user interface system as a whole).
User Needs	General statements about what your users need the device to do expressed in the language they would use.

4. REFERENCES

References made within this document:

4.1. Internal

- P-0007 Risk Management Procedure
- DOC-0013 User Manual

5. RISK MANAGEMENT PLAN

5.1. Planned Activities

All safety risk management activities, and the review of these activities, shall be performed during their appropriate phases as specified in the phase checklists and according to P-0007 Risk Management Procedure. Risk control measures shall be verified like any other requirements.

5.2. Safety Risk Identification Methods

The following methods will be used to identify risks related to the device:

- The MAUDE Alerts database shall be reviewed for entries to related FDA product codes.
- Review the FDA's Total Product Life Cycle database for entries to related FDA product codes.
- Perform an FMEA for all identified System Items.
- Step through the various User Needs and identify usability related risks (including evaluating the DOC-0013 User Manual).
- Answer the "Characteristics Related to Safety" questions derived from ISO/TR 24971:2020 Annex A.

Characteristic	**Description of relevance to safety**
Measurements	CT Cardiomegaly performs automated measurements. These measurements are intended to detect certain parameters (E.g., CTR >.5)
Data Input	CT Cardiomegaly takes existing CT scans as input. The quality of the CT scans could potentially affect performance
Information	Information related to safety (as applicable) will be provided in the DOC-0013 User Manual.
Information	CT Cardiomegaly output is contained in a report. There is no user interface with the software. The clinical user will determine the value of the information and what if any clinical actions should be taken.

5.3. Safety Risk Likelihood Levels

The likelihood of a safety risk occurring shall be classified according to these qualitative levels:

Label	**Description**
Improbable (1)	Assumed not to occur or cannot be distinguished from zero.
Remote (2)	Unlikely to occur, but is possible to occur very rarely over the life of the product.

Label	Description
Occasional (3)	Possible for a relative few occurrences over the life of the product.
Probable (4)	Likely to occur multiple times (but not frequently) over the life of the product.
Frequent (5)	Likely to occur frequently or to be experienced continuously over the life of the product.

5.4. Safety Risk Severity Levels

The severity of a safety risk occurring shall be classified according to these qualitative levels:

Label	Description
Negligible (1)	Results in inconvenience or temporary discomfort
Minor (2)	Results in superficial injury or impairment not requiring professional medical care
Moderate (3)	Results in temporary, non-serious injury requiring professional medical care
Serious (4)	Results in life-threatening injury, permanent impairment or injury which requires medical/surgical intervention to preclude permanent impairment/damage
Catastrophic (5)	Results in death

5.5. Safety Risk Acceptability Levels

Label	Description
Acceptable	The risk level is acceptable, but all risk controls that are viable or capable of being put into practice without reducing the effectiveness of the medical device (e.g., introducing confusing UI or process, adding unnecessary labeling warnings) should be implemented.

Label	Description
Attempt to Mitigate	The risk level is acceptable, but all risk controls that are viable or capable of being put into practice without reducing the effectiveness of the medical device (e.g., introducing confusing UI or process, adding too many unnecessary labeling warnings) must be implemented.
Unacceptable	The risk is unacceptable and must be mitigated. If it can't be mitigated further, then a risk/benefit-analysis must be performed.

5.6. Safety Risk Acceptability Matrix

Likelihood \ Severity	Negligible (1)	Minor(2)	Moderate (3)	Serious (4)	Catastrophic (5)
Frequent (5)	Attempt to Mitigate	Attempt to Mitigate	Unacceptable	Unacceptable	Unacceptable
Probable (4)	Attempt to Mitigate	Attempt to Mitigate	Attempt to Mitigate	Unacceptable	Unacceptable
Occasional (3)	Acceptable	Attempt to Mitigate	Attempt to Mitigate	Attempt to Mitigate	Unacceptable
Remote (2)	Acceptable	Acceptable	Attempt to Mitigate	Attempt to Mitigate	Attempt to Mitigate
Improbable (1)	Acceptable	Acceptable	Attempt to Mitigate	Attempt to Mitigate	Attempt to Mitigate

5.7. Safety Risk Overall Acceptability Criteria

Residual risks are evaluated by the same method and with the same criteria for risk acceptability as the initial risks. The residual risk will be determined to be acceptable or unacceptable. When unacceptable, further risk control options must be investigated. If further risk control is not practicable, a benefit-risk analysis shall be performed and the result documented.

5.8. Methods of Obtaining Post-Production Information

Post-production safety feedback shall be collected using these activities:

- Collecting feedback from customers
- Collecting problem reports/complaints from customers
- Monitoring the MAUDE Alerts database

6. SECURITY RISK MANAGEMENT PLAN

Security risks will be tracked and assessed using the safety risk likelihood, severity, and acceptability levels, adapted as appropriate.

6.1. Security Risk Identifications Methods

The following methods will be used to identify risks related to the device:

- Reviewing vulnerability databases for software dependencies in the SBOM