



www.softwarecpr.com

20 Berkshire Drive
Winchester, MA 01890
781-721-2921

Copyright

© Copyright 2008 Crisis Prevention and Recovery, LLC. (CPRLLC), all rights reserved. SoftwareCPR is a division of Crisis Prevention and Recovery, LLC and the SoftwareCPR® logo is a registered trademark.

SoftwareCPR® authorizes its clients and SoftwareCPR®.com subscribers use of this document for internal review and training. **Any other use or dissemination of this document is expressly prohibited** without the written authorization of SoftwareCPR®. Individual original FDA documents in their original form without SoftwareCPR® annotations are public information and may be shared without restriction.

Legal Disclaimer

The training document that follows **should only be applied in the appropriate context with oversight by regulatory and software professionals with direct knowledge and experience with the topics presented.** The document should not be used as a cookbook since it is not adequate for some situations and may be excessive for others.

While SoftwareCPR® attempts to ensure the accuracy of information presented, no guarantees are made since regulatory interpretations and enforcement practices are constantly changing, and are not entirely uniform in their application.

Disclaimer of Warranties: The information is provided AS IS, without warranties of any kind. CPRLLC does not represent or warrant that any information or data provided herein is suitable for a particular purpose. CPRLLC hereby disclaims and negates any and all warranties, whether express or implied, relating to such information and data, including the warranties of merchantability and fitness for a particular purpose.

Standard Operating Procedure

This is a training and is not intended to be implemented without further analysis and tailoring. It was prepared by Brian Pate of SoftwareCPR®

Risk Management

<doc id>

Table of Contents

TABLE OF CONTENTS	2
1. PURPOSE AND SCOPE.....	3
2. REFERENCES	3
3. DEFINITIONS	3
4. ROLES AND RESPONSIBILITIES	4
5. INPUTS.....	4
6. PROCEDURE	4
6.1 RISK ANALYSIS	4
6.1.1 Identify Intended Use	4
6.1.2 Identification of Known and Foreseeable Hazards	5
6.1.3 Identification of Failure Paths.....	6
6.2 RISK EVALUATION	6
6.3 RISK CONTROL	6
6.3.1 Inherently Safe Design.....	6
6.3.2 Design and Process Mitigations.....	6
6.3.3 External Mitigations.....	7
6.4 OVERALL RESIDUAL RISK EVALUATION	7
6.5 POST PRODUCTION RISK MANAGEMENT.....	7
6.5.1 Discovery of New Hazards or Failure Paths	7
6.5.2 Evaluation of Risk as Part of Failure Investigation.....	7
7. OUTPUTS.....	8
7.1 RISK ANALYSIS REPORT	8
7.1.1 Failure Path with Pre-Mitigation Analysis Table.....	8
7.1.2 Risk Control Measures Table.....	8
7.1.3 Residual Risk/Post-Mitigation Analysis Table.....	9
7.2 RISK MANAGEMENT PLAN.....	9
7.3 RISK-BENEFIT ANALYSIS REPORT	10
7.3.1 Risk Benefit Approvals	10
APPENDIX A: RISK ANALYSIS RATING SCALE.....	11

1. Purpose and Scope

< describe what processes and the scope of activities will be subject to this procedure >

2. References

Reference	Document Name
ISO14971:2000	Medical devices - Risk management - Part 1: Application of risk analysis to medical devices
TIR32:2004	Medical device software risk management

3. Definitions

Term	Reference	Definition
ALARP	ISO14971	Acronym for “As Low As Reasonably Practicable”
CAPA	(Internal)	Corrective Actions and Preventive Actions
Failure Path	(Internal)	The causes or combinations of causes that can lead to the top level event (in the case of an FTA) or the event of interest, i.e. results in hazard.
Foreseeable Misuse	(Internal)	Use of the medical device in a manner the manufacturer did not intend but could have reasonably predicted as a consequence of human behavior.
Harm	ISO14971	Physical injury or damage to the health of people, or damage to property or the environment
Hazard	ISO14971	Potential source of harm
Hazard Analysis	IEC60601-1-4	Identification of hazards and their initiating causes
Hazardous Situation	ISO14971	Circumstance in which people, property or the environment are exposed to one or more hazard(s)
Intended Use	ISO14971	Use of a product, process or service in accordance with the specifications, instructions and information provided by the manufacturer
Manufacturer	ISO14971	Natural or legal person with responsibility for the design, manufacture, packaging or labeling of a medical device, assembling a system, or adapting a medical device before it is placed on the market and/or put into service, regardless of whether these operations are carried out by that person himself or on his behalf by a third party
Residual Risk	ISO14971	Risk remaining after protective measures have been taken
Risk	ISO14971	Combination of the probability of occurrence of harm and the severity of that harm
Risk Analysis	ISO14971	Systematic use of available information to identify hazards and to estimate the risk
Risk Assessment	ISO14971	Overall process comprising a risk analysis and a risk evaluation

Term	Reference	Definition
Risk Control Measure	AAMI TIR32:2004	AAMI TIR32:2004 defines “protective measures” as the actions taken to reduce the risk of hazards and ultimately the risk of harm. These actions may be preventive, corrective, or mitigative. Although the term mitigation is sometimes used as a synonym for protective measure, mitigation has a more specific meaning as indicated above. Protective measures or risk control measures are the generic terms used to describe the steps taken to reduce risk.
Risk Management	ISO14971	Systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating and controlling risk
Risk Management File	(Internal)	A portion of the Design History File that contains documentation and records of the risk management activities undertaken during the project.
Safety	ISO14971	Freedom from unacceptable risk
Severity	ISO14971	Measure of the possible consequences of a hazard.
Verification	ISO14971	Confirmation by examination and provision of objective evidence that specified requirements have been fulfilled

4. Roles and Responsibilities

< Describe who will make this procedure work. Hint: describe roles, not actual persons. The assignment of roles to people can be handled separately. >

5. Inputs

This section identifies possible inputs to the Risk Management process. The < team > shall determine the appropriate methodologies for identifying potential failure modes in the medical device. ...

< This is where you want to describe all of the inputs to the risk analysis process, e.g. FTA. >

6. Procedure

6.1 Risk Analysis

6.1.1 Identify Intended Use

For the particular medical device or accessory being considered, describe the intended use/intended purpose and any reasonably foreseeable misuse. The < team > shall list all those qualitative and quantitative characteristics that could affect the safety of the medical device and, where appropriate, their defined limits. These records shall be maintained in the risk management file.

ISO14971 lists many questions that should be considered during the analysis process. They are:

- ☐ What is the intended use/intended purpose and how is the medical device to be used?
- ☐ Is the medical device intended to be used by individuals with various skill levels and cultural backgrounds?
- ☐ What role is the medical device intended to play in the diagnosis, prevention, monitoring, treatment or alleviation of disease, compensation for injury or handicap, replacement or modification of anatomy, or control of conception?

- ☐ Is the medical device life sustaining or life supporting?
- ☐ Is special intervention necessary in the case of failure of the medical device?
- ☐ Are there special concerns about interface design features that could contribute to inadvertent use error
- ☐ Is the medical device intended to contact the patient or other persons?
- ☐ What materials and/or components are incorporated in the medical device or are used with, or are in contact with, the medical device?
- ☐ Is energy delivered to and/or extracted from the patient?
- ☐ Are substances delivered to and/or extracted from the patient?
- ☐ Are biological materials processed by the medical device for subsequent re-use?
- ☐ Is the medical device supplied sterile or intended to be sterilized by the user, or are other microbiological controls applicable?
- ☐ Is the medical device intended to be routinely cleaned and disinfected by the user?
- ☐ Is the medical device intended to modify the patient environment?
- ☐ Are measurements taken?
- ☐ Is the medical device interpretative?
- ☐ Is the medical device intended for use in conjunction with medicines or other medical technologies?
- ☐ Are there unwanted outputs of energy or substances?
- ☐ Is the medical device susceptible to environmental influences?
- ☐ Does the medical device influence the environment?
- ☐ Are there essential consumables or accessories associated with the medical device?
- ☐ Is maintenance and/or calibration necessary?
- ☐ Does the medical device contain software?
- ☐ Does the medical device have a restricted shelf-life?
- ☐ Factors that should be considered include labeling or indicators and the disposal of such medical devices.
- ☐ Are there any delayed and/or long-term use effects?
- ☐ To what mechanical forces will the medical device be subjected?
- ☐ What determines the lifetime of the medical device?
- ☐ Is the medical device intended for single use?
- ☐ Is safe decommissioning or disposal of the medical device necessary?
- ☐ Does installation or use of the medical device require special training?
- ☐ Will new manufacturing processes need to be established or introduced?
- ☐ Is successful application of the medical device critically dependent on human factors such as the user interface?
- ☐ Does the medical device have connecting parts or accessories?
- ☐ Does the medical device have a control interface?
- ☐ Does the medical device display information?
- ☐ Is the medical device controlled by a menu?
- ☐ Is the medical device intended to be mobile or portable?

6.1.2 Identification of Known and Foreseeable Hazards

The < team > shall compile a list of known or foreseeable hazards associated with the medical device in both normal and fault conditions. Previously recognized hazards shall be identified. This list shall be included in the Risk Analysis and maintained in the risk management file.

A variety of sources, including those listed in Section 5 (Inputs), should be used to identify possible hazards/risks associated with the type of device/monitoring parameters. These sources might include:

- ☐ Articles published in medical device and clinical journals
- ☐ Medical Device Reports (MDRs) and product recalls reported to the FDA
- ☐ Emergency Care Research Institute (ECRI) publications
- ☐ Standards and guidance documents
- ☐ Device quality assurance plans and information generated by design verification and validation, including design reviews, bench testing and clinical studies

For each clinical hazard identified, the Clinical Representative, working with the < team >, shall assign a severity rating using the “Severity of Injury” list in Appendix A of this document.

6.1.3 Identification of Failure Paths

Once the hazards for the intended use environment have been identified, the < team > shall evaluate the product design to determine all failure paths that could possibly lead to one or more of the hazards. The < team > shall utilize the inputs to this process as listed in Section 5 (Inputs). Annex D of ISO14971:2000 should be reviewed by the engineering team to stimulate thinking for this activity.

For software related failure analysis, the < team > should involve an adequate number of software engineers and system engineers so that multiple levels of analysis occur, ranging from the hardware interface layer to the user interface layer.

6.2 Risk Evaluation

Using Appendix A, the < team > shall evaluate each failure path identified prior to any risk control measures being applied. In some cases, this may be a bit confusing since many risk control measures are common design practice and may be planned for the design prior to the risk management process. However, this pre-mitigation analysis is useful in that it provides the < team > with a “baseline” RPN score so that the effect of the risk control measures is more quantifiable.

During the risk management process, the < team > may perform the risk evaluation for a particular failure path multiple times as mitigations are added, further developed, or removed. This process culminates with a final, residual risk evaluation. Refer to section 6.4 (Overall Residual Risk Evaluation).

6.3 Risk Control

For each failure path that requires risk reduction (or further risk reduction), the < team > team, working with the project team technical staff, shall identify and apply appropriate and effective risk control measures. These risk control measures may take the forms described in the sections below.

6.3.1 Inherently Safe Design

Obviously, the most effective risk control measures are those that are “inherently safe,” that is, the possibility of the hazard is eliminated altogether. Early in the product concept phase of the project, the designers should consider the potential hazards and how they might be eliminated through inherent design. Some examples of inherently safe design might be:

- ☐ Non-conductive signal leads eliminate the possibility of electrical shock (hardware)
- ☐ Static declaration of data stores as opposed to dynamic allocation/delete to eliminate the possibility of memory fragmentation or memory leaks (software)

6.3.2 Design and Process Mitigations

When inherently safe design approach is not possible or feasible, the designers shall identify and apply specific and general design and/or process mitigations. Specific mitigations are targeted at explicit defects. For example, a redundant pressure transducer is designed into a non-invasive blood pressure control circuit to mitigate the hazard presented if the primary pressure transducer fails.

General mitigations are meant to “catch” indeterminate causal chains of failure. The designers should identify key points in the design where effective mitigations could be placed to “catch” and prevent further propagation of the failure. For example, a current limiting resistor is designed into the circuit for a heater signal (electronic thermometer) that comes into contact with the patient. Several failure modes could lead to the signal experiencing excessive current, but the resistor will limit current in any case.

The designers shall also identify and ensure that appropriate, on-going process mitigations are in place to verify proper functioning of design mitigations in the manufacturing process, if appropriate. Very strong

design mitigations can be negated by the lack of traceable requirements driven to the manufacturing process. For example, a watchdog circuit in a finished good may have a failure that goes undetected in the factory. Thus, the risk reduction offered by the watchdog function is not present in the product in the field. This scenario might have been avoided if the designers ensured that the watchdog function was tested in manufacturing prior to shipment.

This activity of the risk management process is critical and should begin early in the project. The < team > should ensure that all design and process mitigations undergo appropriate design review.

6.3.3 External Mitigations

The final safeguard for controlling risk is external mitigations. External mitigations are any person, process, or activity in the intended care environment that may reduce the probability of the hazard occurring. Most commonly this involves the user of the medical device. By providing the user with instructions for use, warning, cautions, training, and other information, the user can become a key element in reducing the risk. However, this should be a last resort in the risk control process.

One area that should receive particular attention from the design team is that of the user interface for the medical device. A usability study may be a useful activity to not only identify potential use errors, but also to help the designers to understand the mindset and model of the user and then to use that information in the design of the user interface. A well understood user interface will improve safety.

6.4 Overall Residual Risk Evaluation

The risk analysis process is complete if:

- ☐ the post-mitigation RPN for all failure paths is in region 1 (Negligible) or 2 (Acceptable), and
- ☐ any item in risk region 2 is determined to be “ALARP”.

The < team > shall close the risk analysis process and schedule the final review/approval.

If there are any failure paths that the post-mitigation RPN evaluates to region 3 (Undesirable; Objectionable) with no further mitigation possible, refer to section 7.3 (Risk-Benefit Analysis Report).

Note: For failure paths that the post-mitigation RPN evaluates to region 4 (Unacceptable), this procedure has no mechanism for completion of the risk analysis. A major redesign may be required and/or reevaluation of the intended use.

6.5 Post Production Risk Management

6.5.1 Discovery of New Hazards or Failure Paths

If, after production start, new information is received, through field reports, MDR, or any other source, that indicate that the medical device poses new hazards or new failure paths (not reported in the risk analysis), or that the current risk analysis scoring is in error, the < team > shall re-initiate the risk management process, as described in sections 6.2 (Risk Evaluation), 6.3 (Risk Control), and 6.4 (Overall Residual Risk Evaluation), and provide an updated risk analysis for the medical device.

6.5.2 Evaluation of Risk as Part of Failure Investigation

A key activity for failure investigations and an input to the CAPA process is a risk evaluation. In a similar manner in which this procedure is applied to new product development, the potential hazard arising from the reported failure should be evaluated. The < team > shall determine if reported failure mode follows a failure path that is already documented in the risk analysis for that medical product. If the failure path already exists, the < team > shall determine if the risk control measures performed as expected. The < team > shall evaluate whether updates should be made to the existing risk analysis. If the failure path is determined to be

new, the risk analysis shall be updated as described in section 6.5.1 (Discovery of New Hazards or Failure Paths). In either case, the calculated RPN and resulting risk region shall be included in the risk analysis section of the failure analysis report.

If the failure investigation leads to the inclusion of a new failure path or if the risk evaluation leads to the inclusion of a new mitigation, the < team > shall work with the failure investigation to determine why the gap existed in the risk analysis and if any similar gaps exist with the other hazards and failure paths in the risk analysis.

7. Outputs

7.1 Risk Analysis Report

The risk analysis shall be recorded in a set of three tables. These three tables correspond roughly to the phases of developing the risk analysis during the product development lifecycle.

7.1.1 Failure Path with Pre-Mitigation Analysis Table

The following table describes each of the columns to be used in the Failure Path with Pre-Mitigation Analysis Table:

Column Heading	Explanation
Failure Path	Unique number to be used across all tables to reference the particular failure path being analyzed. These numbers shall remain unique throughout the lifecycle of the product.
Clinical Hazard (CH)	This column identifies the possible clinical effect resulting from the failure being analyzed.
System Failure	This is the result of the defect or error propagation that has the potential to cause harm.
Cause N+1	Higher level causes in the causal chain.
Cause N+2	Lower level causes in the causal chain.
Severity	The worse case effect of the hazard prior to any design or process mitigations.
Pre-Mitigation Probability (Hardware only)	The probability that the fault will occur, resulting in the hazard. Frequency and duration of exposure will affect probability of fault.
Pre-Mitigation Susceptibility (Software only)	The likelihood that the set of inputs and machine state will occur. The measure of predisposition or resistance against defect.
Pre-Mitigation Vulnerability (Software only)	The likelihood that the software defect will propagate to a system failure. The measure of inherit system design resistance to error propagation.
Pre-Mitigation RPN	Risk probability number calculation prior to any design or process mitigations.

7.1.2 Risk Control Measures Table

The following table describes each of the columns to be used in the Risk Control Measures Table:

Column Heading	Explanation
Failure Path	Unique number to be used across all tables to reference the particular failure path being analyzed. These numbers shall remain unique throughout the lifecycle of the product.
Design Mitigations - Narrow	Lower level or specific risk control measures designed to either lower the probability of hardware defects, or Susceptibility of software defects.

Design Mitigations - Broad	Higher level or non-specific risk control measures designed into the device or its labeling that lower either the probability of a hardware defect, or likelihood that a software defect will propagate to a system failure.
External Mitigation	Processes, procedures, or other systems, outside of the system design, located between the last point of device control and the hazard that affect the likelihood that the defect will propagate to a system failure.
Process Mitigations	On-going provisions in the manufacturing processes or otherwise to ensure that the risk control measures remain intact or in place, e.g. incoming inspection, HIPOT, etc.

7.1.3 Residual Risk/Post-Mitigation Analysis Table

The following table describes each of the columns to be used in the Residual Risk/Post-Mitigation Table:

Parameter	Explanation
Failure Path	Unique number to be used across all tables to reference the particular failure path being analyzed. These numbers shall remain unique throughout the lifecycle of the product.
Rationale – Reduced Probability	The worse case effect of the hazard prior to any design or process mitigations.
Rationale – Reduced Susceptibility	The likelihood that a caregiver detects the hazardous condition in time to prevent, or reduce the extent, of injury prior to any design or process mitigations.
Rationale – Reduced Vulnerability	The probability that the fault would occur, resulting in the hazard, prior to any design or process mitigations.
Post-Mitigation Probability (Hardware only)	The probability that the fault will occur, taking into account the design and process mitigations.
Post-Mitigation Susceptibility (Software only)	The likelihood that the set of inputs and machine state will occur, taking into account the design and process mitigations.
Post-Mitigation Vulnerability (Software only)	The likelihood that the software defect will propagate to a system failure, taking into account the design and process mitigations.
Post-Mitigation RPN	Risk probability number taking into account any design or process mitigations. Residual risk.

7.2 Risk Management Plan

For the particular medical device or accessory being considered, the < team > shall prepare a Risk Management Plan in accordance with the risk management process. The risk management plan shall be part of the risk management file.

This plan shall include the following:

- ☐ The scope of the plan, identifying and describing the medical device and the life cycle phases for which the plan is applicable;
- ☐ Verification plan;
- ☐ Allocation of responsibilities;
- ☐ Requirements for review of risk management activities; and
- ☐ Criteria for risk acceptability.

If the plan changes during the life cycle of the medical device, a record of the changes shall be maintained in the risk management file.

7.3 Risk-Benefit Analysis Report

If a failure path, even after all reasonable, practical measures have been taken to lower the risk, still results in a risk in Region 3, the < team > may recommend that a formal decision be discussed on whether the risks are outweighed by the benefits. This discussion and resulting decision shall be documented in the Risk-Benefit Report. This report should include adequate and detailed description(s) of the benefits to public health to be gained by the medical device. In addition, the report should provide in-depth detail of the failure path, the causes, and the rationale for RPN scoring. Finally, an analysis section should build the case for releasing, or not releasing, the medical device as designed.

In general, the greater the risk score, the more extensive and detailed the report should be. An existing Risk-Benefit Report may be referenced, in place of conducting a new one, if appropriate.

Risk-Benefit Reports are generally created at initial product release, but may be created through the CAPA process for released products.

There is no “standardized” approach to estimate benefit, so each case must be evaluated individually, in the manner best fitting the situation. Benefit can be estimated from:

- ☐ The performance expected during clinical use,
- ☐ The clinical outcome expected from that performance, and
- ☐ Factors relevant to the risks and benefits of other treatment options. This may not be relevant to all medical devices, and can be interpreted instead as the risks and benefits of NOT having the device available for use.

The following are examples of risk benefit analyses where the benefits have been judged to outweigh the risks:

- ☐ Red blood cell damage by shear stress can occur in blood pumps during Hemodialysis, a common therapy.
- ☐ Burns can occur when using surgical diathermy where the neutral electrode is attached to the patient. Surgical diathermy is very prevalent.
- ☐ The natural cardiac motion of the beating right atrium creates cyclic stresses on the atrial lead wire used with pacemakers, which can lead to metal fatigue.

7.3.1 Risk Benefit Approvals

In addition to the members of the < team >, a Risk-Benefit Report must also be reviewed and approved by:

- ☐ < This should should be extraordinary and beyond normal product release signoff levels. >

Appendix A: Risk Analysis Rating Scale

For **hardware related faults**, two dimensions are evaluated to calculate the Risk Priority Number (RPN) of the resulting hazard. The first rating is Severity. Severity is the worst case effect of the hazard. The second rating for hardware related faults is Probability. The Probability rating should be based on analysis and published data when possible. To calculate RPN for hazards resulting from hardware related faults, simply multiply the severity rating times the probability rating.

Severity of injury

The worse case effect of the hazard.

No adverse health effect	0
Transient, self-limiting illness or minor injury	1
Temporary, but significant impairment, reversible	5
Serious injury, permanent impairment, irreversible	10
Life-threatening, death could occur	38

Probability of fault

The probability that the fault will occur, resulting in the hazard. Frequency and duration of exposure will affect probability of fault.

0	0	0	0
1	1	2.5	5
3	5	13	25
5	10	25	50
19	38	95	190

For **software related faults**, three dimensions are evaluated to calculate the Risk Priority Number (RPN) of the resulting hazard. Again, the first rating is Severity. Severity is identical to how it used for hardware, except here you consider the system failure that results from the software defect or the error propagation from the defect. The second rating is Susceptibility. This rating reflects the likelihood that the software defect will actually occur. The final rating is for Vulnerability. With this rating, the team is evaluating the software design and structure for robustness and resistance to error propagation (will the software system design prevent the software defect from propagating to a system failure). To calculate RPN for hazards resulting from software related faults, multiply the severity rating times the susceptibility rating times the vulnerability rating.

Severity of injury

The worse case effect of the hazard.

Susceptibility

The likelihood that the set of inputs and machine state will occur. The measure of predisposition or resistance against defect.

Vulnerability

The likelihood that the software defect will propagate to a system failure. The measure of inherit system design resistance to error propagation.

No adverse health effect	0	Very Unlikely to Occur	0.7	Very Unlikely to Propagate	0.75	0	0	0
Transient, self-limiting illness or minor injury	1	Unlikely to Occur	1.0			1	1	2
Temporary, but significant impairment, reversible	5	Likely to Occur	2.0			3	4	8
Serious injury, permanent impairment, irreversible	10					5	8	15
Life-threatening, death could occur	38					20	29	57

Unlikely to Propagate	1.1	0	0	0
		1	1	2
		4	6	11
		8	11	22
		29	42	84

Likely to Propagate	3.0	0	0	0
		2	3	6
		11	15	30
		21	30	60
		80	114	228

The following risk regions are defined for classifying failure paths:

Risk Region	Overall Risk Categories	Post Mitigation RPN	Project Team Action/Response
1	Negligible Risk	< 5	No further risk control measures required.
2	Acceptable Risk (if ALARP)	5 to 19	Acceptable risk if RPN is “as low as reasonably practicable.”
3	Undesirable; Objectionable	20 to 59	If no further risk control measure can be applied, a Risk-Benefit Report must be written, evaluated, and approved by appropriate clinical representatives.
4	Unacceptable under any circumstances	>= 60	Benefit is too low compared to risk.



www.softwarecpr.com

20 Berkshire Drive
Winchester, MA 01890
781-721-2921

Copyright

© Copyright 2008 Crisis Prevention and Recovery, LLC. (CPRLLC), all rights reserved. SoftwareCPR is a division of Crisis Prevention and Recovery, LLC and the SoftwareCPR® logo is a registered trademark.

SoftwareCPR® authorizes its clients and SoftwareCPR®.com subscribers use of this document for internal review and training. **Any other use or dissemination of this document is expressly prohibited** without the written authorization of SoftwareCPR®. Individual original FDA documents in their original form without SoftwareCPR® annotations are public information and may be shared without restriction.

Legal Disclaimer

The training document that follows **should only be applied in the appropriate context with oversight by regulatory and software professionals with direct knowledge and experience with the topics presented.** The document should not be used as a cookbook since it is not adequate for some situations and may be excessive for others.

While SoftwareCPR® attempts to ensure the accuracy of information presented, no guarantees are made since regulatory interpretations and enforcement practices are constantly changing, and are not entirely uniform in their application.

Disclaimer of Warranties: The information is provided AS IS, without warranties of any kind. CPRLLC does not represent or warrant that any information or data provided herein is suitable for a particular purpose. CPRLLC hereby disclaims and negates any and all warranties, whether express or implied, relating to such information and data, including the warranties of merchantability and fitness for a particular purpose.