Medical Device Risk Management

April 23, 2019

PREPARED FOR:
FDA News 16th Annual Medical Device Congress

PRESENTED BY:
Eric Henry
Senior Quality Systems and Compliance Consultant
“It does not do to leave a live dragon out of your calculations, if you live near one.”

- J.R.R. Tolkien -

“Named must your fear be before banish it you can.”

- Yoda -
Problem(s)

• How do medical device manufacturers determine of their products are safe?
• Risk must be managed throughout the entire product lifecycle (pre-market and post-market)

Solution

• ISO wanted a standard (ISO/TC 210, WG 4) and IEC wanted to put risk management into IEC 60601 (IEC/SC 62A, WG 15) → ISO/IEC JWG 1
• Combined standard released in 2000 as EN ISO 14971:2000
The Current State of EN ISO 14971

From then until now...

**EN ISO 14971:2007**
- Currently in force
- Recognized by US FDA
- Changes
  - Focus on Management Responsibility
  - Tightening of ALARP
  - Post-market monitoring introduced
  - Disclosure of residual risk

**EN ISO 14971:2012**
- “Corrected” version of 2007
- Harmonized Standard in EU (not recognized by US FDA)
- Changes (Z Annexes – moved to front)
  - Requirement to reduce negligible risks
  - RBA required for all risks
  - ALARP replaced by AFAP
  - No risk reduction due to information for safety

“Consensus Paper for the Interpretation and Application of Annexes Z in EN ISO 14971: 2012” published October 2014 to address the controversies surrounding implementation of the “Z” annexes in 14971:2012
The Current State of EN ISO 14971

...and next...

EN ISO 14971:2019 under development since 2016 and revises EN ISO 14971:2007 directly

62A/1282/CDV (Committee Draft for Vote) released for voting July 2018 and approved November 2018

Publication August-September 2019
Significant Changes to EN ISO 14971:2007 (...and what this means to you) (1)

Definition of “Harm” Revised

- Removed the word “physical”
- “injury or damage to the health of people, or damage to property or the environment”
- 2019 language in Forward: “It is explained that the process described in ISO 14971 can be used for managing all types of risks associated with medical devices, including those related to data and systems security.”
- 2019 Annex A.2.1: “Risks related to data and systems security are specifically mentioned in the scope, to avoid any misunderstanding that a separate process would be needed to manage security risks.”
- Impact: Cybersecurity and privacy risks may now be considered “harm” subject to 14971
Significant Changes to EN ISO 14971:2007 (...and what this means to you) (2)

“Benefit” Defined

Alignment with MEDDEV and FDA Guidance

• “positive impact or desirable outcome of the use of a medical device on the health of an individual, or a positive impact on patient management or public health | Note 1 to entry: Benefits can include positive impact on clinical outcome, the patient’s quality of life, outcomes related to diagnosis, positive impact from diagnostic devices on clinical outcomes, or public health impact.”

• Better alignment with MEDDEV 2.7.1/1 Revision 4 (“Clinical Evaluation: A Guide for Manufacturers and Notified Bodies Under Directives 93/42/EEC and 90/385/EEC”) and FDA Guidance (e.g. “Factors to Consider Regarding Benefit-Risk in Medical Device Product Availability, Compliance, and Enforcement Decisions”)

• Impact: May alter the objective of Risk-Benefit Analysis, with new definition
Significant Changes to EN ISO 14971:2007 (...and what this means to you) (3)

**RBA -> BRA**

Benefit – Risk Analysis Elaborated

- 2007 language: “If this evidence does not support the conclusion that the medical benefits outweigh the residual risk, then the risk remains unacceptable.”
- 2019 language: “If this evidence does not support the conclusion that the medical benefits outweigh this residual risk, then the manufacturer may consider modifying the medical device or its intended use. Otherwise, this risk remains unacceptable.”
- Annex D moved to TR 24971
- Annex ZA language removed (required RBA in all instances – regardless of acceptability)
- **Impact**: (1) BRA now clearly driven by acceptability; (2) by adding the design change language and thus linking to post-market data, continuous evaluation of benefit-risk is necessary (recurring theme)
Intentional and Unintentional in Scope

- “use of a product or system in a way not intended by the manufacturer, but which can result from readily predictable human behavior | Note 1 to entry: Readily predictable human behaviour includes the behaviour of all types of users, e.g. lay and professional users. | Note 2 to entry: Reasonably foreseeable misuse can be intentional or unintentional.”
- Definition includes use error, as well as reasonably foreseeable abnormal misuse
- **Impact**: This may expand the instances of reasonably foreseeable misuse included in risk analysis
Significant Changes to EN ISO 14971:2007 (...and what this means to you) (5)

Risk Control Measures Clarified

Same Priorities, with Clarified Definitions

• “Inherently safe design and manufacture”
• “Information for safety and, where appropriate, training”
• Impact: Design transfer activities and training activities may be necessary in risk control measures before evaluating residual risk
Significant Changes to EN ISO 14971:2007 (...and what this means to you) (6)

Better Alignment with IEC 62366-1

- Added definition of “accompanying documentation” (for disclosure of residual risk), which includes “instructions for use, technical description, installation manual, quick reference guide, … auditory, visual, or tactile materials and multiple media types”

- Definition of “use error” broadened beyond acts or omissions leading to a “different medical device response” to now include any action (or lack of action), which results in a “different result than that intended”

- Considerations for intended use elaborated (i.e. “intended medical indication, patient population, part of the body or type of tissue interacted with, user profile, use environment, and operating principle”) and tied to use specifications, as defined by 62366

- **Impact**: More use considerations may be needed during risk analysis and risk control implementation
Significant Changes to EN ISO 14971:2007 (...and what this means to you) (7)

ALARP

It’s back!

• 2007 language: “The as-low-as-reasonably-practicable approach can be used as part of risk control options analysis (6.2). Risks for which the probability cannot be estimated would normally use the as-low-as-reasonably-practicable approach.”

• 2012 Annex Z language: “Accordingly, manufacturers and Notified Bodies may not apply the ALARP concept with regard to economic considerations.” (Used MDD language as justification)

• 2014 NB Interpretation: “This disregard of economic considerations when reducing risk is not coherent with the Medical Device Directives’ objective as stated in, for example, the following recital of Directive 93/42/EEC”

• 2019 language: “The manufacturer’s policy for establishing criteria for risk acceptability can define the approaches to risk control, for example reducing risk as low as reasonably practicable, reducing risk as low as reasonably achievable, or reducing risk as far as possible without adversely affecting the benefit-risk ratio.”

• Impact: If the organization has moved too far down the “as far as possible” road, consider re-evaluating using a reasonable “as low as reasonably practicable” approach.
Significant Changes to EN ISO 14971:2007 (...and what this means to you) (8)

Residual Risk Clarified

- Unacceptable residual risks now drive “consideration” of additional risk controls, where 2007 language required “application” of additional risk controls (Mandate to consider benefit vs. risk stronger, when evaluating unacceptable residual risk)
- Unacceptable risk disclosure consideration removed from individual residual risk section and kept in overall residual risk section
- Impact: (1) benefit-risk analysis may need to include more discussion of unacceptable residual risks; (2) current disclosure statements may now be more systemic, as opposed to line-by-line discussions of individual unacceptable residual risks
Expanded Post-production Activities

- Post-market surveillance: Clarified sources of data to be reviewed (i.e. production, user, installation, maintenance, supply chain, state-of-the-art)
- What are you looking for? (new hazards / hazardous situations, altered risk profile, changes in state-of-the-art)
- What is the outcome of post-market surveillance? (risk profile re-evaluation, design changes, management evaluation of the risk management process)
- Impact: Risk management process may now need more detail regarding the handling of post-production data and the outcome of reviews thus linking to process improvements and other elements of the QMS (be clear on the feedback loop)
14971 in the Era of EU MDR (1)

### Risk Management Process
- Specific risk management process elements mandated (i.e. risk management plan, risk analysis, risk estimation/evaluation, risk controls, post-market monitoring, risk re-evaluation)
- Risk controls language almost identical to 14971

### ALARP?
- “As low as reasonably practicable” language included in discussion of chemical, physical, and biological risks (Annex I, Section 10.2)
- Risk reduction clearly addressed in terms of acceptability (Annex I, Sections 4 and 10.2)
- “As far as possible” included regarding risk reduction in design and manufacture (Annex I, Section 4(a)) and use-related risks (Annex I, Section 5(a))
14971 in the Era of EU MDR (2)

### Residual Risk
- **14971:** “If the overall residual risk is judged acceptable, the manufacturer shall decide which residual risks to disclose and what information is necessary to include in the accompanying documentation in order to disclose those residual risks.”
- **EU MDR:** “Manufacturers shall inform users of any residual risks.”

### Post-market Monitoring
- “evaluate the impact of information from the production phase and, in particular, from the post-market surveillance system, on hazards and the frequency of occurrence thereof…”
- This may drive greater consideration of $P_1$ (probability of hazardous situation) / $P_2$ (probability of causing harm) method of evaluating probability since many current methods assume occurrence of the hazardous situation leads to harm
“Software ANOMALIES in a particular VERSION of software will be present in all copies of that software.”

“However, the probability of a software ANOMALY leading to a software failure is very difficult to estimate, because of the random nature of the inputs to each separate copy of the software.”

“No consensus exists for a method of estimating the probability of occurrence of a software failure. When software is present in a sequence of events leading to a HAZARDOUS SITUATION, the probability of the software failure occurring cannot be considered in estimating the RISK for the HAZARDOUS SITUATION. In such cases, considering a worse case probability is appropriate, and the probability for the software failure occurring should be set to 1.”

“In many cases, estimating the probability of occurrence of HARM may not be possible, and the RISK should be evaluated on the basis of the SEVERITY of the HARM alone. RISK ESTIMATION in these cases should be focused on the SEVERITY of the HARM resulting from the HAZARDOUS SITUATION.”
A Brief Discussion of Software Risk Management (2)

I respectfully disagree…

• Dependence on severity alone inevitably leads to over-mitigating software-related hazardous situations

• The initial intent of “probability” in the standard included likelihood, but there were translation issues, which prevented the use of this word

• The use of $P_1$ and $P_2$ can deal with the mostly deterministic nature of software, while resurrecting the idea of likelihood into risk analysis (Note: $P$ alone often assumes a $P_2$ of 1, which likely overestimates actual probability of harm)
### A Brief Discussion of Software Risk Management (3)

<table>
<thead>
<tr>
<th>Level</th>
<th>Probability of Hazardous Situation</th>
<th>Likelihood of Hazardous Situation (software only)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Quantitative P1</td>
<td>Qualitative P1</td>
</tr>
<tr>
<td>Level 5</td>
<td>1 to &gt; 0.01</td>
<td>Event can be replicated repeatedly and/or is likely to occur regularly or many times during the life of the product under the specified operating conditions of the device. (Data sources may include engineering judgment, experience with similar devices, etc.)</td>
</tr>
<tr>
<td></td>
<td>(&gt; 1 in 100)</td>
<td></td>
</tr>
<tr>
<td>Level 4</td>
<td>0.01 to &gt; 0.001</td>
<td>Event can be replicated and/or is likely to occur periodically or several times during the life of the product under the specified operating conditions of the device. (Data sources may include engineering judgment, experience with similar devices, etc.)</td>
</tr>
<tr>
<td></td>
<td>(1 in 100 ≥ 1 in 1000)</td>
<td></td>
</tr>
<tr>
<td>Level 3</td>
<td>0.001 to &gt; 0.0001</td>
<td>Event occurs occasionally during the life of the product under the specified operating conditions of the device, where two means for protection against the hazardous situation have simultaneously failed OR where the function / activity leading to the hazardous situation is exercised occasionally. (Data sources may include engineering judgment, experience with similar devices, etc.)</td>
</tr>
<tr>
<td></td>
<td>(1 in 1000 ≥ Rate &gt; 1 in 10,000)</td>
<td></td>
</tr>
<tr>
<td>Level 2</td>
<td>0.0001 to &gt; 0.00001</td>
<td>Event occurs infrequently during the life of the product under the specified operating conditions of the device, where multiple (more than two) means for protection against the hazardous situation have simultaneously failed OR where the function / activity leading to the hazardous situation is exercised infrequently. (Data sources may include engineering judgment, experience with similar devices, etc.)</td>
</tr>
<tr>
<td></td>
<td>(1 in 10,000 ≥ Rate &gt; 1 in 100,000)</td>
<td></td>
</tr>
<tr>
<td>Level 1</td>
<td>≤ 0.00001 (≤ 1 in 100,000)</td>
<td>Event is not reproducible and/or cannot be replicated under the specified operating conditions of the device. (Data sources may include engineering judgment, experience with similar devices, etc.)</td>
</tr>
</tbody>
</table>

**Note:** For the purposes of compliance to IEC 62304:2006 / AMD 1:2015, \( P_1 \) is assumed to be 100% for hazardous situations, where software is the primary cause. On that assumption, the “Level” in this table is then determined based on the Likelihood of the hazardous situation during intended use and foreseeable misuse.
### A Brief Discussion of Software Risk Management (4)  
**Software Drilldown**

<table>
<thead>
<tr>
<th>Level</th>
<th>Likelihood of Hazardous Situation (software only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 5</td>
<td>This probability is associated with unanticipated results that occur frequently with normal use of the device.</td>
</tr>
<tr>
<td>Level 4</td>
<td>This probability is associated with a single operator action or event, or a function that is exercised periodically by the majority of users.</td>
</tr>
<tr>
<td>Level 3</td>
<td>This probability is associated with two specific sequential or simultaneous operator actions or events, or a function that is exercised occasionally by the majority of users.</td>
</tr>
<tr>
<td>Level 2</td>
<td>This probability is associated with infrequent, unanticipated results associated with operation of the device, or as the result of a multiple-step sequence of operator actions or events that are unusual.</td>
</tr>
<tr>
<td>Level 1</td>
<td>Occurrences in this category are generally, upon investigation, found to be non-reproducible, or cannot be properly investigated due to lack of definitive information.</td>
</tr>
</tbody>
</table>

**Note:** For the purposes of compliance to IEC 62304:2006 / AMD 1:2015, \( P_1 \) is assumed to be 100% for hazardous situations, where software is the primary cause. On that assumption, the “Level” in this table is then determined based on the Likelihood of the hazardous situation during intended use and foreseeable misuse.
A word of caution...

**Watch over-use of probability tables... especially in post-market**

**Actual Case:**

- Design issue resulting in frequent servicing causes nine serious injuries (including one death) among service staff over 18 months
- Four CAPAs are requested and submitted to the CAPA Review Board for consideration over this period
- All Four CAPAs are rejected since risk analysis for this issue shows a low probability and a risk profile of “acceptable”

**Moral:**

- Using pre-market estimates of risk to drive investigations, containment, corrections, and corrective actions around post-market data and events (especially serious injuries / death) may lead to significant impacts on the safety of your device
- Real-time and periodic updates of risk analyses (and risk profiles) are necessary based on post-market data and events (Statistics evaluating actual vs. predicted are also helpful)
- Investigations, containments, corrections, corrective actions, and feedback to risk management related to post-market adverse events are expected by the US FDA and are now codified in the EU MDR
Questions?