Welcome to the webinar

How to optimize your medical device risk management with ISO 14971

Navin Dewagan & Lola Furlong

Qualio

DHS

Today’s agenda

01 Why ISO 14971 matters to the FDA

02 Aligning your strategies

03 Optimizing the ISO 14971 lifecycle

04 Continuous ISO 14971 compliance with Qualio

05 Q&A

Qualio

Today’s hosts

Navin Dewagan
CEO
Digital Health Solutions

Lola Furlong
Senior Quality Success Manager
Qualio

Qualio

Quick poll

Qualio

Quick poll

Qualio

What is today about?

Moving beyond checkbox risk management

Building a risk management file that withstands audits and inspections

Making ISO 14971 a practical lifecycle risk management tool

Designing great medical device products that serve patients and clinical users

Qualio

1. Why ISO 14971 matters to the FDA

Qualio

Why ISO 14971 is critical for FDA-regulated devices

- Foundation for demonstrating safety and effectiveness
  - Supports FDA's reasonable assurance determination

- Evaluated through design controls and the DHF (*or MDF after February 2026!*)
  - Risk management is assessed via design inputs, V&V and labeling

- Weak risk management creates regulatory and patient risk
  - Drives FDA findings, additional information requests and delays
  - Leads to post-market issues, complaints and recalls

***Key message**: FDA does not approve risk files. FDA evaluates whether your risk management supports safe and effective device design.*

Qualio

2. Aligning your strategies

Risk management: strategic tool, not constraint!

- Regulatory strategy sets the rules of the game
  - Intended use, classification, submission type and evidence expectations

- Risk management operationalizes regulatory strategy
  - Identifies which risks must be controlled, justified or avoided
  - Informs design choices, development scope and timelines

- Product roadmap is built on risk-informed decisions
  - What features to include or defer
  - Which markets and indications to pursue first
  - How to balance speed, evidence and safety

***Key message**: Risk management executes regulatory strategy and guides product roadmap decisions*

Qualio

Example: SaMD/AI clinical decision support

- Regulatory strategy not clearly defined
  - Intended use written to appear non-device
  - CDS exemption assumed without risk-based justification

- Risk management misapplied
  - Clinical decision impact underestimated
  - Software and algorithm risks not fully characterized

- FDA outcome when CDS exemption does not apply
  - Product determined to be regulated SaMD
  - Risk management and design controls had to be rebuilt

***Key message**: This is what happens when risk analysis is disconnected from intended use*

Qualio

Example: hardware device intended use expansion

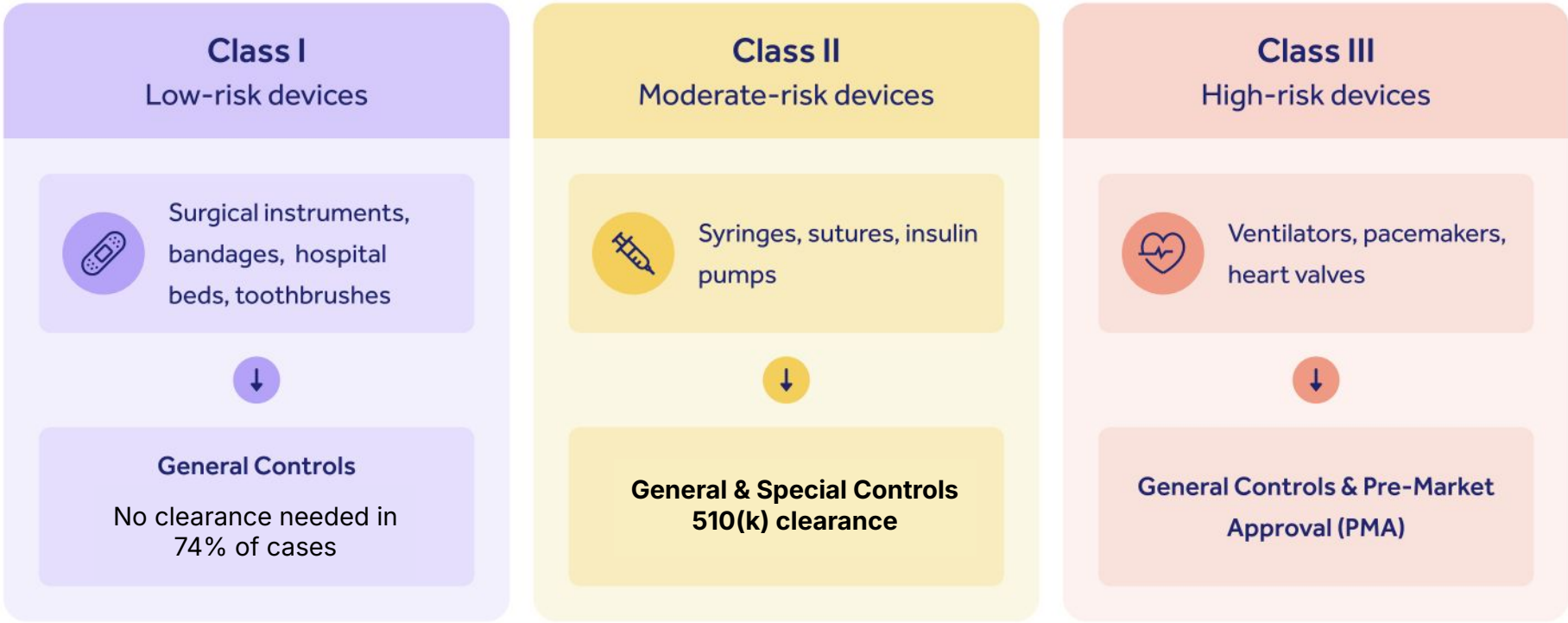
- Regulatory change not fully assessed
  - Intended use expanded to new users or environments
  - Impact on safety assumptions not clearly evaluated

- Risk analysis misapplied
  - Use related hazards not re-identified
  - Severity and probability underestimated for new context
  - Usability and environment of use not fully addressed

- FDA outcome
  - Change determined to significantly affect safety or effectiveness
  - New 510(k) submission required

***Key message**: Changes in intended use invalidate prior risk assumptions and require updated risk analysis to support FDA decisions*

Regulatory pathway drives risk expectations



***Key message**: Your regulatory pathway determines how rigorous your risk analysis must be*

Qualio

Top risk mistakes

1. **Inconsistent intended use across the DHF**

   Intended use differs between risk files, design inputs, labeling and submissions

2. **Risk analysis not grounded in actual use**

   Template-driven hazards not tied to clinical workflow
   Severity and likelihood not justified in context of use

3. **Weak linkage between risk controls and V&V**

   Risk controls not traced to verification or validation evidence
   Effectiveness of controls not demonstrated

4. **Postmarket data not feeding back into risk management**

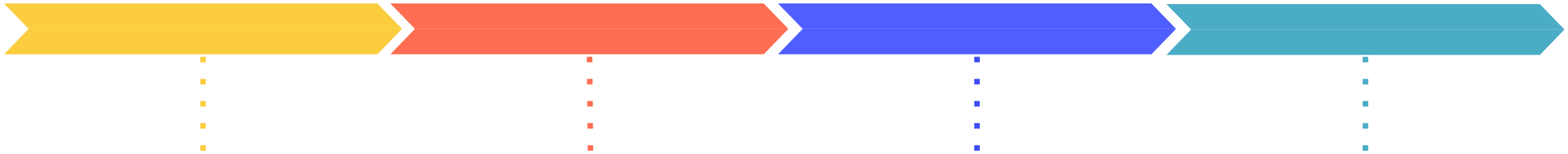
   Complaints, CAPAs and vigilance data not reflected in updated risk analysis

***Key message**: Most FDA findings are driven by inconsistency and weak justification, not necessarily missing documents!*

Qualio

3. Optimizing the ISO 14971 lifecycle

ISO 14971 lifecycle reviewed by FDA



Risk management planning

- Defines intended use, risk acceptability, and decision criteria
- Establishes how risks link to design controls and evidence

Risk analysis & evaluation

- Identifies hazards based on actual use and foreseeable misuse
- Evaluates severity and probability in clinical context

Risk control & verification

- Implements design and process controls to reduce risk
- Verifies and validates effectiveness of risk controls

Production & post-market

- Monitors complaints, CAPAs, and real-world use
- Feeds new info back into ongoing risk analysis

***Key message**: The FDA evaluates risk management across your entire device lifecycle, not as a one-time activity*

Qualio

Using hazard analysis for effective dFMEA

- Hazard analysis sets the safety context
  - Identifies hazards based on intended use and foreseeable misuse
  - Establishes initial severity based on potential patient harm
- Severity determination guides design focus
  - High severity hazards demand early attention
  - Helps engineers prioritize what must be designed out versus controlled
- dFMEA builds on hazard analysis
  - Failure modes are evaluated in the context of identified hazards
  - Severity ratings should align with patient impact, not component failure
- Risk controls flow from hazard severity
  - High severity drives inherent design controls first
  - Lower severity may be addressed through protective measures or information for safety

***Key message**: Strong hazard analysis ensures dFMEA focuses on the right risks & controls*

4 tips for optimized hazard analysis

Qualio

1. **Anchor hazard analysis to intended use *and* foreseeable misuse**

- **Identify hazards based on real clinical use and environments**
- **Consider foreseeable misuse driven by users, workflow, and operating conditions**

2. Define hazards at the use level, *not* the component level

- Focus on hazardous situations that can lead to patient harm
- Avoid generic, template-driven, or purely component-based hazards

Qualio

3. Identify hazards across all relevant domains

- Hardware, software, and system behavior
- Human factors and use related hazards
- Cybersecurity hazards when loss of integrity, availability, or control can impact patient safety

4. Establish hazard severity based on potential patient harm

- Set severity independent of likelihood or attack probability
- Ensure severity reflects worst-case clinical outcome consistent with intended use

Key message: *Hazard analysis defines what must be controlled before selecting controls or performing FMEA*

Qualio

Software and cybersecurity are FDA patient safety concerns

Most medical devices rely on software and connectivity

- Software controls core device functionality and clinical logic
- Connectivity expands the operating environment and risk surface

Qualio

Software and cybersecurity are FDA patient safety concerns

Cybersecurity failures can create hazardous situations

- Loss of availability can delay or interrupt therapy
- Loss of integrity can result in incorrect or unsafe device behavior

Qualio

Software and cybersecurity are FDA patient safety concerns

FDA treats cybersecurity as a safety issue, not an IT issue

- Cyber risks are evaluated when they can impact patient safety
- Cybersecurity must be addressed through hazard analysis and risk controls

***Key message**: When cybersecurity can affect device behavior or availability, it **must** be managed under ISO 14971*

Qualio

Integrated software, cybersecurity & usability risks

Software failures

- Incorrect logic, timing or state handling can lead to hazardous situations

Cybersecurity vulnerabilities

- Loss of availability, integrity or control can alter device behavior
- Cyber events can trigger or amplify safety hazards

Use errors

- User interaction, workflow and cognitive load can all contribute to harm
- Poor usability can increase the likelihood or severity of hazardous situations

Not in isolation!

- Real-world safety events often result from interaction between software, cybersecurity and usability
- FDA evaluates how these risks combine in actual use

Qualio

Integrated software, cybersecurity & usability risks

***Key message**: Effective risk management requires addressing interacting risks, not isolated failure modes*

Qualio

Example: FDA view of a connected device hazard

- Multiple contributing causes
  - Software calculation error affects device output
  - Cybersecurity interruption impacts availability or data integrity
  - User misinterprets alarms due to interface or workflow
- FDA evaluates the combined effect
  - Failures interact across software, cybersecurity and usability
  - Individual issues compound rather than occur independently
- Hazardous situation
  - Delayed, incorrect, or missed therapy delivery
- Patient harm risk
  - Potential for serious clinical consequences depending on intended use

***Key message**: FDA evaluates system-level hazardous situations, not isolated failure modes*

Residual risk and risk-benefit analysis

Integrates all residual risks

Considers remaining risks after all reasonable controls are applied

Includes software, cybersecurity, usability, and use-related residual risks

Documents justified trade-offs

Explains why additional risk reduction is not feasible or would compromise intended use

Demonstrates that risk control decisions were deliberate and evidence-based

Clinical benefit supports risk acceptability

Weighs residual risk against demonstrated clinical benefit

Supports FDA's determination of reasonable assurance of safety and effectiveness

***Key message**: Benefit-risk analysis is where FDA expects risk management decisions to be explicitly justified*

What the FDA expects to see

✅ Objective evidence supporting risk decisions
- V&V data demonstrating effectiveness of risk controls
- Evidence aligned to identified hazards and hazardous situations

✅ Traceability across the DHF/MDF
- Clear linkage from hazards to risk controls to V&V results
- Consistent traceability across risk files, design inputs, and labeling

✅ Consistent intended use across all documents
- Intended use aligned between risk management, submissions, IFU, and marketing claims
- No gaps between stated use and analyzed risk

✅ Post-market feedback incorporated into risk management
- Complaints, CAPAs and real-world use data reviewed and assessed
- Risk analysis updated when new hazards or trends are identified

***Key message**: The FDA evaluates the consistency of your safety story across the **entire** design and post-market lifecycle*

Qualio

Key takeaways

1. ISO 14971 supports reasonable assurance of safety and effectiveness

Risk management underpins the FDA's safety and effectiveness determination

2. Intended use drives FDA risk expectations

Intended use defines hazard scope, severity and evidence expectations

3. Integrated risk management is expected

Software, cybersecurity, usability and use-related risks must all be addressed together

Qualio

4. Strong risk management enables efficient FDA review

Clear hazard analysis, traceability and justification reduce questions and rework

Qualio

Key message:

Strong risk management does not slow your FDA review.

Weak risk management always does!

Qualio

4. Continuous ISO 14971 compliance with Qualio

Qualio

Qualio

qualio.com/demo-ci

Qualio

Q&A

Qualio

Thank you!