ISO 14971 Medical Device Risk Management

by Nick Clark | Published April 25, 2026

Regulatory Framework

ISO 14971:2019, the third edition of the standard, replaced ISO 14971:2007 and was published in December 2019 with concurrent harmonization activity under the EU MDR and IVDR (Regulation (EU) 2017/746). The 2019 revision sharpened the distinction between risk and benefit-risk, refined the definition of state-of-the-art, and aligned the standard with the EU MDR's requirement that risks be reduced "as far as possible" rather than "as low as reasonably practicable." The companion technical report ISO/TR 24971:2020 provides guidance on application, including detailed worked examples for software-of-medical-device, in vitro diagnostic devices, and medical device cybersecurity.

Under the EU MDR, ISO 14971 is the practical pathway to satisfying Annex I General Safety and Performance Requirements 1-9, which require manufacturers to establish, document, implement, and maintain a risk management system, to identify and analyze known and foreseeable hazards, to estimate and evaluate associated risks, to eliminate or control identified risks, and to evaluate the impact of information from the production phase and from the post-market surveillance system on hazards and risks. EU MDR Articles 83-86 (post-market surveillance system, PMS plan, PMS report, periodic safety update report) and Articles 87-92 (vigilance, incident reporting, field safety corrective actions) bind

the risk-management process to mandatory regulatory reporting on timelines measured in days, not quarters.

The FDA's QMSR final rule, with a February 2, 2026 compliance date, incorporates ISO 13485:2016 by reference, and ISO 13485 in turn binds the QMS to ISO 14971's risk-management process. The FDA's September 2023 final guidance on Cybersecurity in Medical Devices (Quality System Considerations and Content of Premarket Submissions) explicitly extends ISO 14971's hazard analysis into security risk, requiring that exploitable vulnerabilities be analyzed under the risk management process and that SBOM provision and post-market vulnerability monitoring be addressed throughout the device lifecycle. AAMI TIR57 and IEC 81001-5-1:2021 operationalize the cybersecurity-risk integration. The combined regulatory force is that ISO 14971 risk management is now a continuous, evidence-driven discipline with security risk as a first-class hazard category.

Architectural Requirement

ISO 14971:2019 defines the risk management process across Clauses 4 through 10. Clause 4 establishes the general requirements (risk management process, management responsibilities, competence of personnel, risk management plan, risk management file). Clause 5 mandates risk analysis. Clause 6 mandates risk evaluation. Clause 7 mandates risk control through inherently safe design, protective measures, and information for safety, with verification of risk-control implementation and effectiveness. Clause 8 mandates evaluation of overall residual risk. Clause 9 mandates risk management review prior to commercial distribution. Clause 10 — the architectural inflection point — mandates production and post-production activities, including the systematic review of post-production information for relevance to safety.

Clause 10.1 requires that the manufacturer establish, document, and maintain a system to actively collect and review information about the medical device in the

production and post-production phases. Clause 10.2 specifies that the information collected shall be evaluated for possible relevance to safety, including new or revised hazards, risks no longer acceptable, changes in the state of the art, or changes that affect the validity of previous risk-management decisions. Clause 10.3 requires that, where the risk-management decisions are affected, the manufacturer shall reassess and, if necessary, take action. The design history file and the risk management file are not static documents — they are living artifacts that must be updated in response to fielded-device evidence.

For a connected fleet of 50,000 infusion pumps, 200,000 continuous glucose monitors, or 5,000,000 implantable cardiac devices, the Clause 10 obligation cannot be satisfied without a continuous, per-device evidentiary stream. The evidentiary stream must support cryptographic attestation of device identity (so that a telemetry record is provably from the device it claims to be from), device integrity (so that the firmware producing the telemetry has not been tampered with), and SBOM provenance (so that a newly-disclosed vulnerability in a transitive dependency can be matched against the deployed component inventory of the field). PUF-grounded device identity, tamper-evident telemetry, and SBOM attestation are not nice-to-have features — they are the architectural floor of ISO 14971 Clause 10 satisfaction.

Why Procedural Compliance Fails

Procedural ISO 14971 implementations satisfy the documentation-of-procedures letter of the standard while failing its evidentiary spirit. A typical post-production information procedure references "complaint logs," "service records," "MAUDE database review," "literature review," and "vigilance reports" as inputs. Each input is a curated artifact produced after an event, by a human, with no structural binding to the device that experienced the event. When a notified body asks during an MDR audit what the firmware version was on the specific pacemaker that delivered an inappropriate shock three months ago, the complaint-log

answer is insufficient — the manufacturer needs cryptographically-grounded device-state evidence at the moment of the event.

Bolt-on fleet-monitoring tooling produces telemetry without the integrity guarantees the regulatory regime demands. A typical IoT-platform deployment streams telemetry from device to cloud across a TLS channel, stores it in a time-series database, and presents it through a dashboard. None of these steps establish, in the legal sense required by ISO 14971 Clause 10, that the telemetry is authentic, that the device producing it was running approved firmware, or that the SBOM under which the telemetry was produced matches the SBOM declared in the design history file. When a vulnerability is disclosed in a transitive dependency, the fleet-monitoring platform cannot answer the question "which devices in the field are running the affected component" with anything stronger than a best-effort inventory.

The cybersecurity-risk integration introduced by AAMI TIR57, IEC 81001-5-1, and the FDA's September 2023 guidance compounds the procedural failure. A risk-management file that lists "exploitation of unauthenticated network interface" as a hazard must, under Clause 10, be reassessed when post-production information indicates that the hazard's likelihood or severity has changed. Without device-integrity attestation, the manufacturer cannot determine whether the hazard has actually been exploited in the field; without SBOM attestation, the manufacturer cannot determine whether a newly-disclosed CVE is exploitable on the deployed firmware. Procedural compliance produces a paper risk-management file that is structurally divorced from the field.

What the Health-Monitoring Primitive Provides

The health-monitoring fleet primitive provides four architectural services that map directly onto ISO 14971 Clause 10. First, PUF-grounded device identity — a Physical Unclonable Function rooted in silicon process variation produces a per-device identity that cannot be cloned, transferred, or forged, and that anchors

every telemetry record to a provably-unique device. The PUF identity is the cryptographic substrate that makes a telemetry record admissible as evidence of the specific fielded device's behavior at a specific time.

Second, device-integrity attestation. At each telemetry emission, the device produces a measured-boot attestation signed under its PUF-derived key, binding the telemetry record to the firmware image, configuration, and SBOM under which it was produced. Tamper-evident logging ensures that any attempt to alter the record after the fact is detectable. The combined effect is a telemetry stream whose every record is provably from a known device, running a known firmware, with a known SBOM, at a known time — the evidentiary substance ISO 14971 Clause 10 presupposes.

Third, zero-trust device management. The fleet is governed under a zero-trust posture in which every device interaction (firmware update, configuration change, telemetry query, field-service action) is authenticated, authorized, and logged with the same five-property structure that anchors ordinary telemetry. Field safety corrective actions under EU MDR Article 89 are executed as zero-trust operations, producing chained evidence of which devices received the corrective firmware, when, and under whose authority. Fourth, SBOM attestation. Each firmware release is published with an attested SBOM (CycloneDX or SPDX) bound by signature to the release; each fielded device's measured-boot attestation references the SBOM under which it is operating; vulnerability disclosure is matched against the live deployed-component inventory by direct query rather than by inventory reconstruction.

Compliance Mapping

ISO 14971 Clauses 4-9 are largely procedural and are satisfied by the existing risk management file, design history file, and risk management plan. The architectural lift is in Clause 10. Clause 10.1 (collection of post-production information) maps onto the fleet's telemetry stream, with each device's PUF-

attested telemetry record serving as primary post-production evidence. Clause 10.2 (review for relevance to safety) maps onto continuous query against the telemetry stream and the SBOM-attested deployed-component inventory, with newly-disclosed vulnerabilities (CVE feeds, ICS-CERT advisories, manufacturer disclosures) automatically matched against the live fleet.

Clause 10.3 (action where risk-management decisions are affected) maps onto zero-trust field actions — firmware updates, configuration changes, device deactivation — each producing a chained record bound to the originating risk-management decision. EU MDR Article 89 (field safety corrective actions) and FDA 21 CFR 806 (medical device correction and removal reports) reporting is satisfied by direct query against the field-action chain. The risk management file becomes a query interface over the live fleet rather than a document that drifts from the field.

The cybersecurity-risk integration maps onto SBOM attestation and device-integrity attestation. AAMI TIR57 hazard analysis for security threats is updated continuously based on tamper-evident telemetry; IEC 81001-5-1 lifecycle security activities are executed as zero-trust operations with chained evidence; the FDA's September 2023 guidance post-market vulnerability monitoring obligation is satisfied by continuous CVE-to-SBOM matching against the live fleet inventory. The design history file's risk management section, the technical documentation submitted under EU MDR Annex II, and the FDA premarket submission's cybersecurity content all reference the same architectural primitive.

Adoption Pathway

Adoption proceeds in three phases. Phase one provisions PUF-grounded identity and measured-boot attestation in new device designs and in firmware updates to fielded devices where silicon support exists. Devices without PUF support are anchored using TPM-backed identity as a transitional measure. The risk management plan is updated to reference the new evidentiary substrate; the risk

management file's Clause 10 procedure is revised to reflect telemetry-driven post-production information.

Phase two integrates SBOM attestation into the build pipeline and the firmware-release process, with each release carrying an attested CycloneDX SBOM bound to the firmware image by signature. The deployed-component inventory becomes a live query against attested telemetry rather than a spreadsheet maintained by hand. Vulnerability response — CVE-to-SBOM matching, exploitability analysis under ISO 14971 hazard analysis, field corrective-action planning — is executed against the live inventory with chained evidence at each step.

Phase three integrates zero-trust device management into field-service workflows, with every device interaction producing chained evidence under the device's PUF-rooted identity. The risk management file becomes a continuously-updated artifact whose contents are queryable rather than narrative; notified-body audits, FDA inspections under the QMSR, and EU MDR vigilance reviews are satisfied by query rather than by document reconstruction. Subsequent regulatory evolution — EU AI Act provisions for medical AI/ML systems, FDA's emerging predetermined change control plan framework, IEC 62304 amendments — accommodates without rebuild because the architectural primitive does not depend on the specific regime.