DHF Impact and Actions Recommendation – ISO 62083:2026

Gap Assessment: ISO 62083:2026 versus ISO 62083:2010

Document Type: Design History File (DHF) Impact Analysis

Standard Reference: ISO 62083:2026 – Medical device software – Requirements for the safety of radiotherapy treatment planning systems

Date: June 28, 2026

Revision: 01

1. Executive Summary

ISO 62083:2026 introduces major new and expanded compliance expectations for radiotherapy treatment planning systems relative to ISO 62083:2010, with a strong shift toward cybersecurity, usability, transparency, structured risk management, formal approvals, installation control, and traceable algorithm/model governance. The attached gap assessment indicates that the most significant DHF impacts include integration with ISO 13485, IEC 62304, IEC 81001-5-1, and IEC 62366-1; new graded test methodology; installation and environment validation; stronger access-control and backup/recovery requirements; broader patient-identification and data-interface controls; formal approval history controls; expanded algorithm and dose-calculation documentation; and extensive new modelling requirements for external beam, brachytherapy, and light-ion applications.

Key Impact Areas for DHF:

- Integrated quality, software lifecycle, cybersecurity, usability, and risk-management governance.
- New test-grade framework and explicit compliance mapping to each requirement.
- Installation/environment validation and reproducible commissioning checks.
- Expanded IFU warnings, access control, backup/recovery, and unauthorized-activity controls.
- New patient identification, data input/output, interface, and approval-history controls.
- Broader algorithm transparency, dose-calculation safeguards, imaging-dose, radiobiological, and modelling documentation.

This document translates the attached ISO 62083:2026 versus 2010 comparison into a DHF impact-and-actions plan using the same implementation style as the attached DHF reference document.

2. Key Changes Summary

2.1 Integrated quality, security, usability, and risk-management framework

Change: Clause 4.1 is a new requirement that explicitly links radiotherapy treatment planning system safety to ISO 13485, IEC 62304, IEC 81001-5-1, and IEC 62366-1, showing that security, software lifecycle control, usability, and risk management are now expected to operate as an integrated discipline. This represents a fundamental shift beyond the 2010 baseline.

DHF Impact:

- The DHF should show explicit cross-references between design controls, software lifecycle records, cybersecurity risk management, usability engineering, and product risk files.
- Legacy evidence structured only around software functionality or dose-calculation performance will likely need re-indexing to demonstrate integrated compliance.
- Governance documents should identify which standards and internal procedures satisfy each part of the new framework.

Recommended Actions:

Action	Timeline	Owner	Priority
Create a standards cross-reference matrix linking ISO 62083:2026 clauses to ISO 13485, IEC 62304, IEC 81001-5-1, IEC 62366-1, and ISO 14971 records	4 weeks	Regulatory / Quality	Critical
Update software DHF index to show cybersecurity, usability, and software-lifecycle traceability	5 weeks	Software QA / Regulatory	Critical
Review design-control procedures for integrated risk, security, and usability governance	6 weeks	Quality Systems	High

2.2 New test grades, compliance mapping, and installation validation

Change: ISO 62083:2026 adds new test grades A, B, and C, requires explicit compliance statements in the technical description, and introduces installation-specific testing and diagnostic checks that account for software and hardware environment dependencies. The gap assessment treats these as new foundational compliance structures rather than simple procedural refinements.

DHF Impact:

- Verification planning must classify each requirement by test grade and define evidence type, execution conditions, and reproducibility expectations.

- Technical descriptions need direct requirement-to-evidence traceability, rather than relying on narrative compliance summaries.
- Installation qualification, environment qualification, and post-change installation verification become formal DHF evidence domains.

Recommended Actions:

Action	Timeline	Owner	Priority
Build requirement-to-test-grade traceability matrix for all applicable clauses	4 weeks	Test Engineering / Regulatory	Critical
Update technical description template to include explicit compliance declarations and evidence references	4 weeks	Documentation / Regulatory	Critical
Develop installation qualification and environment-change verification protocols	6 weeks	System Test / Field Engineering	Critical
Document hardware/software configurations used in type testing and field validation	5 weeks	Test Engineering	High

2.3 Expanded IFU, unit/format controls, and operational transparency

Change: The 2026 edition significantly expands instructions-for-use content, including warnings about installation limitations, qualified approvals, training, input verification, and software-error reporting. It also refines operational-safety expectations for displayed units, measurement accuracy disclosure, coordinate systems, orientation markers, radiation units, and standardized date/time formatting with radionuclide-related time-zone handling.

DHF Impact:

- IFU and technical documentation will need broader safety messaging and more explicit operational constraints than under the 2010 edition.
- Display/output specifications and verification records must demonstrate unit visibility, coordinate identification, orientation markers, and the required time/date conventions.
- Accuracy disclosures and related cautions should be traceable from software requirements into IFU, UI, and verification outputs.

Recommended Actions:

Action	Timeline	Owner	Priority

Revise IFU to include expanded warnings, training, data-verification, and error-reporting instructions	6 weeks	Technical Writing / Regulatory	Critical
Update software requirements and UI specifications for units, coordinates, orientation markers, and date/time handling	6 weeks	Software Engineering / UX	High
Add verification cases for output formatting, unit visibility, and radionuclide time-zone/date behavior	6 weeks	Test Engineering	High

2.4 Access control, backup/recovery, unauthorized activities, and version-change safety

Change: ISO 62083:2026 strengthens role-based authentication, auto-locking, backup/recovery procedures, risk-based protection against unauthorized activities, and software-version transition controls including backup before deletion, conversion of active-patient plans, archived-plan retrieval, unique configuration identification, and version-compatibility warnings. The gap assessment notes that the new edition replaces older point controls with broader safety- and risk-driven cybersecurity expectations.

DHF Impact:

- Security design inputs and risk controls must now address authentication, inactivity lock, backup/restore, unauthorized activity analysis, version migration, and patient safety during upgrades.
- IFU, administrator documentation, and service documentation need clear backup, restore, and upgrade procedures.
- Verification must include functional and adverse-condition tests for recovery, compatibility, migrated treatment plans, and warnings for incompatible models or data.

Recommended Actions:

Action	Timeline	Owner	Priority
Update cybersecurity and software risk files for authentication, unauthorized activities, backup/recovery, and upgrade hazards	6 weeks	Cybersecurity / Risk Manager	Critical
Create or revise backup/restore and version-migration validation protocols using legacy and archived plan data	8 weeks	Software Test / Validation	Critical
Update IFU and admin guides for backup, restore, auto-lock, configuration ID, and version-transition warnings	6 weeks	Technical Writing / Service Engineering	High