Blog post

DCB Standards vs ISO 14971: What Healthcare IT Deployers in England Need to Know

Downloaded on November 19th, 2026



Introduction

For healthcare organisations in England, deploying new IT systems is a critical process that directly affects patient safety and care quality. Two key standards shape risk management in health IT: the UK's Data Coordination Board (DCB) standards and the internationally recognised ISO 14971 standard. This blog post explains both, compares their relevance, and clarifies what deployers need to do to ensure compliance and safety, particularly focusing on DCB0129 and DCB160.

Understanding DCB Standards: DCB0129 and DCB160 Explained

DCB standards are national standards developed specifically for the NHS healthcare providers in England mandated under the Health and Social Care Act 2012. Their purpose is to ensure that health IT systems are safe.

- DCB0129: This standard sets out the clinical risk management requirements for manufacturers of health IT systems. It asks suppliers to establish a documented process for identifying and managing clinical risks associated with their products, ensuring these risks are reduced to an acceptable level.
- DCB0160: While DCB0129 applies to suppliers, DCB0160 is for those deploying and using health IT systems within care settings. It requires organisations to assess the risks of implementing and using the system in their local environment, documenting how those risks will be managed in day-to-day use.

Overview of ISO 14971: Key Principles and Relevance

ISO 14971 is an international standard for risk management of medical devices, including software and AI as a medical device (SaMD/AIaMD). It guides manufacturers to systematically identify, evaluate, and control risks throughout a product's lifecycle. The standard is widely used across the world and underpins regulatory expectations for medical device safety.

- It focuses on proactive identification and control of hazards.
- It requires ongoing documentation of risk analysis, risk evaluation, control measures, and residual risk communication.

Downloaded on 19/11/2026, for the latest information, check the website as printed documents may be outdated.

- It is globally recognised and referenced in European and UK regulations for medical devices.

Comparing DCB Standards and ISO 14971: Similarities and Differences

Both DCB standards and ISO 14971 share a foundation in systematic risk management and documentation. However, they have distinct focuses and applicability:

- Applicability: DCB standards apply specifically to health IT systems deployed within the NHS in England, while ISO 14971 is for medical devices including SaMD globally.
- Applicability: DCB standards assess risk to patients only, while ISO 14971 assesses all risk including users.
- Focus: DCB0129/0160 cover manufacturer and deployer responsibilities separately. ISO 14971 is primarily for manufacturers, covering the entire product lifecycle.
- Risk Communication: Both require that residual risks are communicated. For DCB0129, this means manufacturers must inform deployers about any transferred risk control measures, mirroring ISO 14971's emphasis on communicating residual risks for medical devices. DCB0160 makes it the deployer's duty to assess and implement these when deploying in their environment.
- Documentation: Both frameworks insist on thorough documentation, but DCB standards provide a clearer split between manufacturer and deployer obligations.
- There is a requirement for a CSO (Clinical safety officer) to be appointed under DCB standards. Within ISO 14971, there is a requirement for appropriate clinical professional to participate in risk management activities and be part of the risk management team however there is no requirement for a CSO.
- ISO 14971 artefacts are proprietary to the manufacturer, and they have no obligation to share these with the deployer organisation. They do have to share the residual risks of their device either within the IFU, manual or the labelling. The DCB0129 Clinical Safety Case Report must be shared by the manufacturer with the deploying organisation. The deploying organisation has a right to ask for these documents from the supplier.

Rights and Responsibilities of Deployers

Requesting DCB0129 Documentation: NHS organisations deploying and/or using health IT systems in England have the right to request the DCB 0129 Clinical Safety Case Report

Downloaded on 19/11/2026, for the latest information, check the website as printed documents may be outdated.

from the manufacturer. This documentation outlines the identified risks and risk controls built into the system as well as any transferred risk control measures. Reviewing it is essential for understanding how the system is designed to protect patient safety as well as ensuring any transferred controls are implemented.

Conducting DCB0160: The responsibility for DCB0160 lies with the deploying organisation. They must assess how the new system will be used in their specific setting, identify any local risks, and plan how these will be managed and mitigated to an acceptable level. This process is the deployer's equivalent of the supplier's DCB0129 process.

DCB0160 ensures that the deployment and use of health IT Systems within their specific environment do not introduce new, unmitigated and unacceptable risks—and it is a mandatory step for any new health IT deployment in NHS settings.

Applicability of DCB to Software Medical Devices

To determine whether the DCB standards apply to Software Medical Devices, we can split them into three categories:

- Software in a Medical Device – DCB does not apply to software embedded within a physical medical device, such as software operating insulin pumps or X-ray machines.
- Software as a Medical Device (SaMD) implemented within or forming part of a health IT system – DCB applies to SaMD, or an accessory to SaMD if it is implemented within or forms part of a health IT system, such as drug interaction checkers within EPMA systems
- Standalone Software as a Medical Device not implemented within health IT system – DCB does not apply to standalone SaMD that is not implemented within or forming part of a health IT system, regardless of whether it is deployed within the NHS.

Reference:
For further details, see the NHS England step-by-step guidance on DCB0129 applicability: NHS Digital Clinical Safety Applicability Guidance.

If I Have Done My ISO 14971, Do I Still Need to Do DCB0129? Is This Duplication?

Short answer:
Yes, you must still undertake DCB0129 if it applies (as outlined above) even if you have already implemented ISO 14971. While both standards share core risk management principles, DCB0129 is a mandatory NHS England requirement with unique obligations that are not fully covered by ISO 14971. Completing both is not duplication but ensures compliance with both international and NHS-specific clinical safety expectations.

Downloaded on 19/11/2026, for the latest information, check the website as printed documents may be outdated.

Why Both Standards Are Required

- **Different Focus and Scope:**
  - ISO 14971 is an international standard for risk management of medical devices, including software, focusing on patient, user, and environmental risks.
  - DCB0129 is specific to the NHS in England, focusing exclusively on clinical risk to patients in health IT systems. It requires a Clinical Safety Officer (CSO) and uses NHS-specific processes.
- **Legal and Regulatory Requirements:**
  - NHS organisations are mandated to comply with DCB0160 for health IT deployments.
  - DCB0129 compliance is routinely checked during NHS procurement and assurance processes.
- **Documentation and Audience:**
  - ISO 14971 produces a Risk Management File, primarily for manufacturers and regulators.
  - DCB0129 requires a Hazard Log and Clinical Safety Case Report, tailored for NHS clinical safety governance and reviewed by a CSO.
- **Key Differences Highlighted in NHS Guidance:**
  - Both standards require systematic risk management and documentation, but DCB0129 introduces NHS-specific obligations, such as the appointment of a CSO and the need to share clinical safety documentation with NHS deployers.
  - DCB0129 is focused on clinical safety in respect to the patient, while ISO 14971 covers broader device safety, including cybersecurity and environmental risks.
- **Approach when both required:**
  - Manufacturers may choose to combine their DCB 0129 and ISO 14971 deliverables within one set of risk management documents or separate the deliverables for each standard into two risk management files. There are pros and cons to each approach.
  - Separating the two ensures easier identification of compliance and gaps, more efficient sharing of DCB documents to deployer organisations and less ambiguity as stakeholders would only view the document set relevant to them

Practical Guidance

- **If you have already completed ISO 14971:**
  - Use your ISO 14971 documentation as a foundation but map it against DCB0129 requirements to identify and fill any gaps.

Downloaded on 19/11/2026, for the latest information, check the website as printed documents may be outdated.

- Prepare a separate Clinical Safety Case and ensure a CSO is involved in the review and sign-off process.
- Ensure your risk management activities and documentation use NHS-specific language and address clinical risks in the patient context.

- **Avoiding Duplication:**
  - While some activities (hazard identification, risk evaluation, documentation) can be leveraged for both standards, you must ensure that all DCB0129-specific requirements are explicitly addressed and documented.

Practical Implications: What Deployers Should Do

1. Always request the DCB0129 documentation from your supplier. Review it to understand the risks and controls already identified.
2. Conduct a DCB0160 assessment for your deployment. Document local risks—such as changes to workflow, user training, or integration with other systems—and how you will manage them.
3. Request any transferred risk control measures from the manufacturer, or any residual risks for software medical devices following ISO 14971.
4. Maintain clear records of your DCB0160 process and ensure all stakeholders are aware of their responsibilities regarding ongoing risk management.

Links and Resources

- DCB0129 Applicability and Guidance
- DCB0160 Guidance
- ISO 14971 Standard Overview

Conclusion: Key Takeaways for Healthcare Deployers in England

Deploying health IT systems in England requires a clear understanding of both national and international risk management standards. DCB0129 and DCB0160 provide a structured, complementary approach for suppliers and deployers within the NHS, while ISO 14971 offers a broader framework for medical devices and software internationally.

 Downloaded on 19/11/2026, for the latest information, check the website as printed documents may be outdated.

Remember: manufacturers are mandated to send the DCB0129 Clinical Safety Case Report to deployers.

Deployers have rights and responsibilities

- Right to request DCB0129 documents
- Responsibility to complete DCB0160 for local risk assessment

Both steps are essential to ensure safe, effective, and compliant digital healthcare delivery. For more on how these standards apply to your project, consult the NHS Digital links above or seek expert clinical safety advice.

Downloaded on 19/11/2026, for the latest information, check the website as printed documents may be outdated.