

DCB0129 vs DCB0160: Clinical Safety Accountability Guide



IG-Smart Ltd · Practical Guide Collection · 25 October 2026

General information and original working aids; not legal advice, certification, clinical authorisation or regulatory approval.
NHS identity appearing in retained illustrative artwork does not imply NHS approval or endorsement.

Use this guide to make a better-evidenced decision. This is general information and an original working aid, not a client-specific legal opinion, certification, clinical safety authorisation or regulatory approval. Apply the relevant jurisdiction, current requirements and competent professional review to your circumstances. Examples are illustrative unless expressly attributed.

Your first three steps

1. Confirm the manufacturer, deployer, product version and intended clinical use.
2. Trace each material hazard from manufacturer evidence into the local workflow.
3. Record accountable safety decisions, limitations and conditions before deployment.

Manufacturer and deployment responsibilities, hazard-evidence handover and proportionate clinical risk management for NHS digital health systems

Executive proposition: A manufacturer's clinical safety file does not discharge a deploying healthcare organisation's duty to evaluate risks in its own workflows, population, configurations and operational setting. Equally, local deployment assessment is not a substitute for the manufacturer's product safety process.

For: HealthTech manufacturers, software suppliers, NHS and care deploying organisations, Clinical Safety Officers (CSOs), CIOs, Medical Directors, clinical informaticians and procurement teams. **Boundary:** This guide provides a decision-oriented explanation and proposed working templates, not a completed DCB compliance assessment, appointed CSO opinion, medical-device classification or regulatory approval.

Executive briefing — the decision before procurement, go-live and change

There are two complementary questions: **Has the manufacturer managed clinical hazards in the design, development, maintenance and release of the health IT system?** And **has the deploying organisation assessed whether the same system can be used safely in its own environment?** The relevant clinical safety documentation should cross this boundary with traceable hazards, assumptions, design mitigations, operating restrictions and open issues.

Published NHS England clinical safety guidance distinguishes manufacturer-side DCB0129 from deploying-organisation DCB0160 responsibilities. A consultation or proposed revision does not replace published requirements. Check the latest NHS England publications before live safety-case use. [S1][S2]

Legal precision: Confirm the current legal applicability, published requirements and organisation type before relying on this guide for a live safety case; do not portray consultation proposals as binding requirements.

1. Why the two standards must be understood together

The manufacturer may design reasonable safeguards for a prescribing workflow, but cannot know every deploying organisation's staffing, interfaces, local formulary, training, fallback or device configuration. The deploying organisation can test its local clinical pathway, but should not be expected to invent manufacturer design decisions or independently reconstruct incomplete product hazard analysis.

The clinical safety assurance chain therefore requires **evidence transfer and local challenge**, not an assumption that purchasing a product transfers all responsibility to either party. This matters particularly for systems supporting triage, diagnostics, referrals, medication, clinical coding, patient identification and AI-supported recommendations.

Clinical Safety Officer competence and authority

NHS England's published digital clinical safety guidance describes a Clinical Safety Officer as a suitably qualified and experienced clinician with current registration with an appropriate professional body relevant to their training and experience, and knowledge of clinical risk management. Confirm the applicable manufacturer and deploying-organisation requirements, the nominated person's registration, competence, availability and authority before relying on their assessment. Manufacturer and deploying-organisation responsibilities remain distinct; each organisation retains its management responsibilities. [S4][S5]

Published-requirements boundary: A consultation or proposed revision does not replace published requirements. Check the latest NHS England publications before live safety-case use. [S1][S2]

Core responsibility comparison

Requirement or activity	Manufacturer / DCB0129 emphasis	Deployer / DCB0160 emphasis	Shared boundary
Intended use	Define product function and limitations	Confirm intended local workflows and patient groups	Verify deployment fits product claims
Clinical hazards	Identify product lifecycle hazards	Identify deployment and context-specific hazards	Handover, reconcile and update
Clinical Safety Officer	Appoint suitably qualified CSO within applicable requirements	Establish appropriately qualified CSO and governance	Resolve escalation channels
Safety case	Document product clinical risk evidence	Document deployment clinical risk evidence	Compare assumptions and residual risks
Hazard log	Maintain relevant product hazards and controls	Maintain local hazards and mitigations	Map linked hazards and ownership
Testing	Verify product safety requirements and changes	Test local use, interfaces, configuration and workflows	Agree evidence criteria
Training	State required user competence and safe instructions	Implement local training and supervision	Confirm usability and restrictions
Change management	Assess releases, patches and system-level changes	Evaluate local configuration, interfaces and workflow changes	Timely notice and reassessment
Incident learning	Investigate product-related safety signals	Triage local patient safety incidents and emerging hazards	Joint analysis where relevant
Go-live	Supply evidence and unresolved product issues	Authorised local deployment decision	No universal supplier "sign-off"

2. The IG-Smart Clinical Hazard Handover Map – eight gates

Gate	Decision question	Minimum evidence	Unresolved issue
C1 Intended purpose	What is the product intended to do, and for whom?	Approved intended-use description	Local use outside claims

Gate	Decision question	Minimum evidence	Unresolved issue
C2 Context	Where and how will it operate?	Clinical workflow, environments, interfaces	Unspecified clinical dependency
C3 Product hazards	What harms were identified in product design?	Manufacturer hazard log and safety case information	Material hazard information absent
C4 Local hazards	What new risk arises from deployment?	Local hazard assessment	No deployer assessment
C5 Controls	Which mitigations actually operate in this configuration?	Testing, SOPs, training, fallback	Unverified critical mitigation
C6 Roles	Who owns each unresolved hazard and control?	Named CSOs, owners, escalation paths	Conflicted or missing owner
C7 Decision	Who can authorise release and with what conditions?	Safety case, exceptions, approving authority	Open unacceptable risk
C8 Lifecycle	What changes force reassessment?	Update notifications, incident and change triggers	No post-go-live monitoring

The model is an IG-Smart working decision tool, not an alternative clinical risk management standard. A checked box cannot override a clinical safety objection or missing critical evidence.

3. What a useful manufacturer's evidence handover contains

Buyers should request a **current clinical safety case report**, a sufficiently informative **hazard log** with status and controls, confirmation of the **CSO's function and sign-off according to applicable requirements**, intended use and contraindications, foreseeable misuse, known limitations, relevant technical and clinical testing, integration/interface risks, release/version identification, training and configuration requirements, and a way to report new hazards.

Not every hazard detail can be distributed without restrictions; agree controlled review and record what was inspected. The handover must still permit the deployer to challenge reliance on a mitigation it cannot reproduce or enforce. Document any differences between development assumptions and the care setting.

Hazard provenance fields

Field	Example of the question to answer
Hazard ID and origin	Manufacturer or local deployment finding?
Clinical harm	What plausible patient harm could occur?
Trigger and sequence	What interaction causes the hazard?
Existing mitigation	Designed, procedural, training or monitoring control?
Control owner	Supplier, deployer or shared?
Verification	Test artefact, representative users, date and limitations?
Residual risk	What remains after mitigation; whose decision?
Open action	Required before deployment or monitored under conditions?
Change sensitivity	Which update, workflow or interface changes affect it?

4. What a deployer must assess in its own context

The deploying organisation should establish clinical sponsorship, identify the real user population, map the end-to-end clinical pathway and failure modes, examine clinical usability and accessibility, verify interfaces, define downtime fallback, assess supervision and training, and record a deployment decision with ownership. For AI-enabled or adaptive tools, consider model/version governance, drift and clinician reliance; the precise additional legal regime requires a separate applicability assessment.

Deployment safety-case contents

1. Intended use and care setting.
2. Scope of organisations, services and technical interfaces.
3. Configuration baseline and local deviations.
4. Product documentation examined and gaps in handover.
5. Local hazard identification and linked manufacturer hazards.
6. Safeguards, user training and clinical workflow controls.
7. Verification and user-acceptance evidence with limitations.
8. Incident response and safe downtime arrangements.
9. Residual risk decision, approving authority and go-live conditions.
10. Post-go-live monitoring, change triggers and next clinical review.

5. Risk scoring: interpret the method, not the number

Use a locally approved clinical risk matrix appropriate to the organisation. A supplier's 20-point internal matrix, an NHS-local five-point method and a different international standards method may use distinct definitions and thresholds. **Numeric outputs are not interchangeable without documented mapping of severity, likelihood, acceptability and decision authority.** For a multi-jurisdictional or AI clinical solution, a more granular model may support analysis, but the deploying organisation's mandated local decision framework must still be respected.

A defensible assessment preserves the narrative **hazard → plausible harm → control → verification → residual uncertainty → decision**, regardless of the arithmetic. No model should manufacture an appearance of objectivity where probability data are not available.

6. Interfaces, vendors and shared workflows

Clinical hazards often arise between systems rather than inside a single product. Reconciliation failures, patient-context errors, wrong-user alerts, time-zone mismatches, unsynchronised observations and degraded connectivity can bypass otherwise strong product controls.

A useful interface assurance handover identifies system owners, version compatibility, data quality checks, responsibilities during outages, alert-handling pathways, safe rollback and clinical validation after configuration changes. Where several NHS bodies exchange data, document cross-organisational escalation instead of assuming every downstream organisation has identical workflows.

7. Illustrative clinical safety cases – fictional examples, not client evidence

E-prescribing integration. Manufacturer testing demonstrates dosage validation, but the deploying organisation discovers local formulary exceptions and a risky overnight downtime procedure. Go-live is conditional on revised procedure, testing, ownership and CSO review.

AI-assisted triage. Product safety materials state that clinicians retain final judgement, but local workflow places model recommendations prominently and disincentivises override. The deployer assesses reliance, staff training, audit logs, affected patient groups and escalation; additional AI, privacy and medical-device questions require separate review.

Remote monitoring. Device data are transmitted reliably under lab conditions but a local network outage can defer clinical alerts. The deployment hazard assessment defines fallback observations, escalation periods, recovery verification and change control.

8. Procurement questions that reveal assurance quality

- Which exact product version and intended-use statement does the safety case cover?
- Who prepared and approved the product hazard log and when?
- Which material clinical hazards remain open and what conditions apply?
- Which mitigations depend on local configuration, staffing or clinical decisions?
- Can the supplier explain why its risk rating transfers to this deployment?
- What evidence exists for interoperability and data-integrity testing?
- What change notification is provided for safety-relevant software releases?
- How are clinical incidents and previously unknown hazards jointly escalated?
- Does the supplier claim DCB0160 compliance on behalf of the NHS organisation?
- Are medical-device and other statutory classifications separately addressed?
- Has the relevant Clinical Safety Officer actually assessed the proposed local deployment?
- What must be revalidated after the next system or workflow change?

9. A one-page clinical safety deployment decision

Product and version: __; **intended use and care setting:** __; **manufacturer evidence reviewed:** __; **deployer hazards added:** __; **unacceptable and conditional risks:** __; **mitigations tested:** __; **CSO involvement:** __; **clinical owner:** __; **decision:** proceed / condition / defer / reject; **approval authority:** __; **post-deployment monitoring:** __; **change triggers:** __.

No signature should be treated as a substitute for unresolved material evidence. A clinical safety case report must communicate its actual limitations rather than produce a blanket “safe” certificate.

10. Frequently asked questions

Does DCB0129 certification mean an NHS trust is ready to deploy? The premise is misleading: assess the manufacturer evidence and local deployment obligations; DCB0129 work does not replace DCB0160.

Does DCB0160 require every supplier to employ the NHS customer's CSO? The deployer and manufacturer have distinct arrangements; roles must be established under the applicable requirements and contracted scope.

Can DTAC substitute for a clinical safety assessment? No. DTAC includes clinical safety criteria but does not automatically complete every manufacturer's or deployer's clinical risk management task.

Does a safety case replace a hazard log? They serve related but distinct purposes; ensure hazards, controls, residual decisions and evidence can be traced.

Can clinical risks be rated only with a supplier's score? The deploying organisation must apply its approved acceptability method with appropriate contextual evidence.

Do clinical risk standards automatically settle UK medical-device status? No. Medical-device classification and regulatory requirements need separate assessment.

What if a manufacturer refuses full safety documentation? Agree appropriately controlled access, record gaps and avoid claiming assurance beyond evidence examined.

Can a CSO approve any unresolved patient harm exposure? Decision authority and acceptable residual risk must follow applicable governance; no sign-off automatically legitimises an unacceptable hazard.

A condition is not a permission slip. Where a clinical safety or legal prerequisite is unresolved, record it as a condition that must be satisfied **before** deployment or the affected use. A procurement deadline, supplier signature or generic risk score cannot authorise an unacceptable hazard. Use the organisation's clinical safety escalation and decision arrangements, not this guide as a clinical instruction.

11. Practical implementation

Use the companion Clinical Safety Handover & Deployment Record to establish product-specific and organisation-specific evidence. Start with the intended-use declaration and local workflow before requesting lengthy evidence sets. Escalate missing CSO competence, material hazards and unresolved safety conditions as blockers, rather than lowering scrutiny to meet a tender deadline.

Related services: [Clinical Safety Consultancy](#), [Clinical Safety Officer Services](#), [DTAC Readiness](#), [HealthTech Governance](#). A Clinical Safety Officer appointment must be expressly agreed for the engagement.

Next step: Submit a Requirement describing the health IT product, relevant NHS setting, current safety artefacts and intended deployment; the firm can determine suitable scoping without promising procurement or go-live approval.

Sources

- [S1] NHS England, National review of clinical risk management standards DCB0129 and DCB0160: supporting information (29 June 2026) <https://www.england.nhs.uk/long-read/national-review-of-clinical-risk-management-standardsdcb0129-and-dcb0160-supporting-information/>
- [S2] NHS England, National review consultation (closed 11 September 2026) <https://www.engage.england.nhs.uk/patient-safety/national-review-of-clinical-risk-management-standards/>
- [S3] NHS England, Patient Safety Strategy progress update, July 2026 <https://www.england.nhs.uk/patient-safety/the-nhs-patient-safety-strategy/nhs-patient-safety-strategy-progress-so-far/>
- [S4] NHS England, Clinical risk management standards: current DCB0129 and DCB0160 specifications and guidance. <https://digital.nhs.uk/services/clinical-safety/clinical-risk-management-standards>
- [S5] NHS England, Digital clinical safety assurance: DCB responsibilities and CSO role. <https://www.england.nhs.uk/long-read/digital-clinical-safety-assurance/>