

NHS Digital Health Procurement Evidence Playbook



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. Define the actual product, version, data flows and deployment.
2. Assign manufacturer, deploying organisation and supplier responsibilities separately.
3. Use the crosswalk to expose evidence gaps before a procurement or deployment decision.

DTAC, DSPT, DCB0129 and DCB0160: an assurance framework for HealthTech suppliers and NHS buyers

For suppliers entering the NHS market from overseas

Start with the intended deployment in England and the buyer's evidence requirements, not the supplier's home country. Existing security reports, privacy assessments or foreign market approvals may be useful evidence, but are not automatic substitutes for the relevant NHS, clinical safety or product requirements. Record what can be reused, the limits of that evidence and the remaining work. Neither this playbook nor consultancy support guarantees acceptance by an NHS buyer.

Executive summary

A successful NHS digital health procurement is not established by collecting four certificates. This guide concerns NHS procurement and health IT assurance in **England**; requirements and commissioning arrangements elsewhere in the UK must be checked separately. Digital Technology Assessment Criteria (DTAC), the Data Security and Protection Toolkit (DSPT), and clinical risk management standards DCB0129 and DCB0160 address different assurance questions. Their applicability, owners and evidence must be established in context.

DTAC examines whether a software-based digital health product meets the relevant baseline criteria across clinical safety, data protection, technical security, interoperability, and usability and accessibility. DSPT assesses an organisation's data security and protection practices where NHS patient information or systems are involved. DCB0129 governs clinical risk management by manufacturers of relevant health IT systems; DCB0160 addresses the safe deployment and use of those systems by health and care organisations. These mechanisms interact, but none automatically substitutes for another. [1][2][3][4]

The essential procurement question is not simply 'Is the supplier compliant?' It is: 'Which requirements apply to this product, organisation and deployment; who owns each risk and control; and what current evidence supports an accountable decision?'

This playbook provides an applicability matrix, accountability map, evidence crosswalk, readiness checklist and executive decision briefing. It is a practical working aid, not an NHS-endorsed assessment, legal determination, certification or guarantee of procurement acceptance.

At a glance: four assurance mechanisms, four different questions

Mechanism	Primary question	Primary accountable party	Illustrative evidence	Boundary to preserve
DTAC	Does the specific digital health product meet the applicable NHS baseline assessment criteria?	Supplier prepares product evidence; NHS buyer/commissioner conducts and records its assessment	Current version-specific DTAC form, supporting documentation, buyer assessment record	Not an all-purpose certificate, medical-device authorisation or substitute for local acceptance
DSPT	Does the relevant organisation demonstrate appropriate data security and protection practices for NHS data/systems?	Each in-scope organisation for its own toolkit submission; buyer checks relevant evidence	Applicable organisational DSPT status, assertions, evidence, remediation records	Organisation-level assurance is not equivalent to product-level DTAC or a DPIA
DCB0129	Has the manufacturer managed clinical hazards associated with creating or maintaining the relevant health IT system?	Manufacturer and its appointed clinical safety leadership	Clinical risk management plan, hazard log, clinical safety case report, release/change records	Manufacturer documentation does not discharge the deployer's local clinical safety obligations
DCB0160	Has the deploying health/care organisation evaluated and managed the clinical risks of using the technology in its own setting?	Deploying organisation and its clinical safety leadership	Local hazard assessment, safety case, training/workflow controls, deployment acceptance and monitoring	Local implementation cannot simply adopt supplier claims without assessing context

Do not conflate product and organisational assurance. The DTAC assessment concerns an applicable digital health technology; a DSPT return concerns the relevant organisation and its current category. Neither constitutes a blanket NHS product endorsement, and the need for each must be determined from the actual supplier, product, buyer and deployment facts. [1][3]

2026 changes to recognise. NHS England introduced a simplified DTAC form in February 2026, with roughly 25% fewer questions; the previous form should no longer be used from **6 April 2026**. The DSPT portal provides **2026–27 version 9 category-specific requirements**; NHS England states a **30 June 2027** submission deadline for that cycle. A consultation or proposed revision does not replace published requirements. Check the official sources and applicable scheme before relying on any historical template. [1][5][6]

1. Start with the product, deployment and data flow - not a checklist

Before requesting documentation, record six facts:

- 1. Intended purpose and clinical effect.** Does the system merely schedule appointments, support clinical decisions, calculate risk, communicate results or influence direct care?
- 2. Legal and operational actors.** Who develops it, supplies it, commissions it, deploys it, hosts it and provides clinical oversight?
- 3. Deployment context.** Is it used in publicly funded health or adult social care in England, in an NHS-connected service, or in a wholly private/wellness context?

4. **Data and connectivity.** Does the organisation access NHS patient information or systems? Which parties are controllers, processors and sub-processors?
5. **Medical-device status.** Could the intended purpose bring the software under MHRA medical-device requirements, in addition to NHS procurement and clinical safety obligations?
6. **Product version and change profile.** Which version, integration, user group, clinical workflow and AI-enabled features are being assessed?

Decision rule: An uncertain answer is an assessment task, not a reason to tick 'not applicable'. Record the uncertainty, accountable owner, evidence needed and date for resolution. NHS England provides a dedicated applicability guide for DCB0129/DCB0160; this playbook does not replace that decision path. [7]

2. Applicability matrix: common scenarios

Legend: **Assess** = determine the actual requirements using official guidance and contract terms; **Likely relevant** = a strong starting presumption, not a blanket legal conclusion; **Conditional** = applies where the organisation/product meets the relevant scope.

Scenario	DTAC	DSPT	DCB0129	DCB0160	Additional check
HealthTech supplier offers clinical workflow software to an NHS trust	Likely relevant to product assessment	Conditional on supplier NHS data/ system access and applicable category	Assess; often relevant for manufacturer of in-scope health IT	Likely relevant to trust deployment	MHRA device status; DPIA; integrations; local risk
NHS trust deploys a third-party system in direct patient care	Likely relevant to acquisition/ assurance	Likely relevant to trust organisation	Request manufacturer's applicable evidence	Likely relevant to trust's own use	Local workflow controls and risk acceptance
IT services provider accesses NHS patient systems but does not manufacture clinical software	Product-dependent; may be outside DTAC scope	Likely relevant to provider's organisation	Conditional , if it manufactures relevant health IT	Conditional , if it deploys/uses in a relevant care setting	Supplier-security, contract and access assurance
Software may qualify as a medical device	Assess alongside medical-device rules	Conditional	Assess under official applicability and product/ integration context	Assess for deployment context	MHRA qualification, classification and additional regulatory evidence
Consumer wellness app with no publicly commissioned care use	Do not assume DTAC applies	Not automatic solely because the product is health-related	Do not assume statutory scope; consider safety good practice	Do not assume statutory scope; consider safety good practice	Intended use, buyer contract and future NHS deployment
AI-supported patient triage or decision support	Likely relevant in an applicable NHS purchase	Conditional	Assess carefully , including model and system hazards	Assess carefully , including local monitoring and clinician interaction	MHRA status, performance, drift and human oversight

Important: Official DCB applicability guidance considers publicly funded care in England, intended use, the effect on direct care, and medical-device status. Suppliers and buyers should document the decision rather than applying the matrix mechanically. [7] The DTAC scope is focused on software-based digital health technologies; its assessment is used alongside other necessary assurance processes. [1]

3. The IG-Smart Procurement Assurance Evidence Chain

A practical **six-gate decision model** for organising evidence, proposed by IG-Smart for this guide. It is **not** an NHS standard or certification scheme.

Gate 1 — Applicability: Identify the product, version, care setting, organisational actors and applicable requirements.

Gate 2 — Accountability: Name the supplier owner, deploying organisation owner, clinical safety leads, information governance decision-maker and procurement decision-maker.

Gate 3 — Evidence: Request current, traceable documents and test results that directly address the applicable requirement.

Gate 4 — Exceptions: Record missing evidence, control gaps, open hazards, remediation actions, unresolved interfaces and contractual dependencies.

Gate 5 — Decision: Put a documented go/conditional-go/defer recommendation before the authorised buyer and safety decision-makers, with explicit limitations and risk ownership.

Gate 6 — Change: Define refresh triggers for product releases, material architecture or AI-model changes, new data flows, incident findings, clinical workflow changes and changes in official requirements.

The differentiator is traceability: every important statement should connect to a named owner, current evidence, an assessed exception and a decision. A green dashboard without that chain is not defensible assurance.

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. Source: <https://service-manual.nhs.uk/standards-and-technology/service-standard-points/16-make-your-service-clinically-safe>

4. Accountability: the manufacturer-to-deployer handover

Activity	Supplier/manufacturer	NHS buyer/commissioner	Deploying health/care organisation
Define intended use and product version	Own and document	Check alignment with purchase	Confirm intended local use and deviations
Complete relevant DTAC evidence	Prepare and maintain	Assess form and supporting evidence	Inform local integration and acceptance decision
Maintain applicable organisational DSPT submission	Own its submission if in scope	Check appropriate supplier assurance	Own its own organisational obligations
Manage manufacture-related clinical hazards (DCB0129)	Lead when applicable; appoint appropriate clinical safety leadership	Request evidence and explain procurement conditions	Assess transfer of hazards, mitigations and residual risks

Activity	Supplier/manufacture	NHS buyer/commissioner	Deploying health/care organisation
Manage local deployment risks (DCB0160)	Explain product limits and required controls	Confirm accountable deployment arrangements	Lead applicable local safety analysis, acceptance and monitoring
Assess controller/processor roles and DPIAs	Supply information and fulfil its legal role	Establish procurement and data-sharing requirements	Own relevant local processing decisions and DPIA responsibilities
Manage security, interfaces and supplier changes	Disclose design, controls, vulnerabilities and changes	Apply supplier due diligence	Verify local configuration, access, resilience and integrations
Accept residual local clinical risk	Cannot unilaterally accept on behalf of deployer	Confirm decision governance	Authorised local decision-makers evaluate and accept within governance arrangements

Clinical safety handover test: Can the deployment lead identify every supplier hazard or mitigation that depends on the buyer's local workflow, staff training, configuration, integration or fallback procedure? If not, the assurance chain is incomplete. NHS England's own API examples show manufacturer-level DCB0129 evidence and deployment-level DCB0160 responsibilities co-existing without transferring risk ownership to NHS England. [8]

5. The evidence crosswalk: what a reviewer should ask for

The examples below are a working request guide. The definitive required documents depend on the current official form, standards, local procurement, contract and product risk. Avoid re-requesting documents that the buyer already holds in an acceptable format.

Evidence domain	Supplier evidence / question	Buyer and deployment challenge
DTAC – clinical safety	Current clinical safety responsibilities; applicable DCB0129 evidence; safety-case and hazard-log references	Are the product boundary, safety assumptions and deployer dependencies clear?
DTAC – data protection	Data-flow map; processing purposes; controller/processor allocation; privacy governance and DPIA support	Are the lawful processing arrangements and local high-risk processing decisions addressed?
DTAC – technical security	Relevant current security assessment, vulnerability and remediation information, secure development and access controls	Does evidence reflect the version, hosting model, integrations and local security requirements?
DTAC – interoperability	Relevant standards, interfaces, data formats, identity, integration tests and constraints	Can the system exchange information safely and correctly in the intended pathway?
DTAC – usability/accessibility	Usability evidence, accessibility evaluation, known limitations and mitigation	Have affected users, clinical workflows and accessibility needs been considered?
DSPT	Correct organisation/category, current version and applicable publication/evidence status	Does the submission apply to this legal entity, scope and NHS access arrangement?
DCB0129	Clinical risk management plan; hazard log; clinical safety case report; CSO arrangements; release controls	Are hazards controlled, exceptions identified and local safety dependencies communicated?

Evidence domain	Supplier evidence / question	Buyer and deployment challenge
DCB0160	Supplier hazard transfer information and implementation prerequisites	Does the deployer have its own local safety case, trained owners, go-live controls and continuing review?
Cross-cutting	Sub-processors; incident escalation; contractual responsibilities; change notices; version history	Can the buyer trace ownership and receive updated evidence when risks or services change?

NHS England makes clinical safety document templates available, including a clinical risk management plan, hazard log and clinical safety case report. These are working aids; completing a template does not itself demonstrate sufficient clinical risk control. [9]

6. Common evidence failures - and how to detect them

Failure 1: A 'DTAC certificate' with no traceable assessment. Ask for the current DTAC form, the product/version assessed, relevant supporting evidence and the buyer's assessment outcome. DTAC is an assessment framework, not a universally issued NHS certificate. [1][2]

Failure 2: An outdated DTAC form. Check the 2026 form rather than reusing material from before the April 2026 transition. [1]

Failure 3: A supplier's DSPT status used as product approval. Verify the organisational scope and current year, but examine product-level controls and local processing separately. [3][5]

Failure 4: A DCB0129 safety case treated as a substitute for DCB0160. Ask the deploying organisation to demonstrate how supplier hazards and local use risks have been assessed. [4][7]

Failure 5: Undefined clinical safety ownership. Record who is accountable for manufacturer and deployer safety activities, including named clinical safety leadership and escalation.

Failure 6: Evidence from the wrong product release. Match technical tests, hazard assessments and assurance records to the deployed build, integration and AI model where applicable.

Failure 7: Unresolved issues hidden inside a 'pass'. Require an exceptions log showing material gaps, owners, mitigations, due dates and decision status.

Failure 8: Security claims without deployment context. Consider identity, privileged access, supplier connectivity, hosting and incident responsibilities in the actual buyer environment.

Failure 9: Medical-device status overlooked. DTAC does not replace MHRA medical-device obligations. An intended-purpose analysis may be necessary for software and AI tools. [10]

Failure 10: No change-control or reassessment triggers. Approval of version A should not silently be assumed to cover a materially different version B.

7. Working checklist: procurement evidence readiness

Use **Complete / Gap / Not applicable (with rationale)** for every line. Evidence must be linked to an owner and a date. The list is an IG-Smart aid, not an official NHS assessment form.

A. Scope and roles

- [] Product name, assessed release/version and intended clinical purpose recorded.

- ☐ NHS buyer, manufacturer, reseller, deployer and hosting parties identified.
- ☐ Data flows, NHS connectivity and intended patient/user groups mapped.
- ☐ Medical-device qualification and classification considered where relevant.
- ☐ Official DTAC and DCB applicability decisions recorded, with reasons.

B. DTAC evidence

- ☐ Latest official DTAC form obtained and completed for the relevant product.
- ☐ Clinical safety evidence and any manufacturer-to-deployer dependencies identified.
- ☐ Data protection evidence and DPIA-support information available.
- ☐ Security evidence and remediation exceptions are current.
- ☐ Interoperability evidence reflects actual interfaces and standards.
- ☐ Usability and accessibility evidence reflects intended users and workflow.
- ☐ Buyer assessment outcome and supplementary requirements recorded.

C. DSPT and information governance

- ☐ In-scope legal entities and applicable DSPT submission categories identified.
- ☐ Relevant DSPT year/version, evidence and published status checked.
- ☐ Supplier and buyer organisational responsibilities distinguished.
- ☐ Controller/processor arrangements, data-sharing terms and local DPIA ownership addressed.

D. Clinical safety and deployment

- ☐ DCB0129 applicability, manufacturer CSO arrangements and evidence checked.
- ☐ Manufacturer hazard log and clinical safety case available where applicable.
- ☐ Transferred hazards and required local controls expressly documented.
- ☐ DCB0160 applicability and deploying-organisation CSO arrangements checked.
- ☐ Local workflow, interfaces, training, incident and fallback risks evaluated.
- ☐ Appropriate local safety and go-live decision recorded.

E. Exceptions and continuing assurance

- ☐ Material gaps have named owners, proportionate mitigations and review dates.
- ☐ Contract terms allocate evidence updates, incidents and change notifications.
- ☐ Reassessment triggers cover product changes, AI updates and changing clinical use.
- ☐ The final procurement recommendation distinguishes evidence complete, accepted exceptions and unresolved blockers.

8. Executive decision briefing: one-page template

Decision: [Proceed / Proceed subject to conditions / Defer pending evidence / Do not proceed]

Board or procurement question	Record for decision-makers
What is being bought and for whom?	Product, version, supplier, buyer, intended users and care setting
What is the intended clinical and data-use boundary?	Intended purpose, direct-care effect, data types and integrations
Which requirements apply?	DTAC, organisational DSPT, DCB0129/DCB0160, MHRA and any buyer-specific requirements, each with an applicability rationale

Board or procurement question	Record for decision-makers
Who owns the decision and the risks?	Named procurement, clinical safety, information governance and cyber accountable roles
What evidence supports readiness?	Linked, dated documentation and assessed results; not supplier assertion alone
What remains unresolved?	Priority exceptions, material residual clinical/data/cyber risks and owner
What conditions must be satisfied before go-live?	Controls, demonstrations, contractual terms, training and formal acceptance
When must assurance be revisited?	Version, AI/model, integration, incident, data-flow and regulatory triggers

Suggested recommendation wording: 'On the evidence reviewed as at [date], the proposed [product/version] has [specified evidence status] against the requirements assessed as applicable. The recommendation is [decision] subject to [conditions]. This is not a guarantee of regulatory compliance, clinical safety or procurement success; accountable parties retain responsibility for their respective obligations.'

9. Two contrasting examples

Scenario A – Clinical decision-support SaaS procured by an NHS trust. The supplier should be prepared to explain its intended clinical purpose, product version, clinical risk management, security, data protection and interoperability evidence. The trust should document its own DTAC assessment, applicable organisational DSPT position, local clinical workflow hazards and DCB0160 obligations. If the software qualifies as a medical device, MHRA requirements must be evaluated in parallel. Neither supplier assurance nor a vendor safety case transfers the trust's local decision responsibilities. [1][4][10]

Scenario B – Administrative SaaS with access to NHS patient information but no direct clinical effect. The organisation's DSPT obligations may still be relevant because of NHS patient data/system access. DTAC and the clinical safety standards cannot be assumed applicable merely because the software is sold to an NHS organisation; assess intended use, product scope, procurement conditions and official guidance. Data protection, supplier security, integration and contractual evidence still matter. [3][7]

10. Questions buyers ask

Is DTAC a certificate that guarantees NHS procurement approval?

No. DTAC is an NHS assessment framework for digital health technologies. A supplier provides the current form and supporting evidence, while buyers assess the product in their own procurement context. Other requirements, including clinical safety, information governance, medical-device regulation and local deployment assurance, may still apply. [1][2]

Does a DSPT submission mean the product is DTAC-ready?

No. DSPT assesses relevant organisational data security and protection practices. DTAC is product-focused across five domains. A current organisational DSPT position can form part of broader assurance, but it does not establish the remaining product or deployment requirements. [1][3]

What is the distinction between DCB0129 and DCB0160?

DCB0129 concerns clinical risk management associated with the manufacture of applicable health IT systems. DCB0160 concerns clinical risk management when applicable systems are deployed, used and maintained by health or care organisations. Both sides need a clear record of their responsibilities and any transferred hazards. [4][7]

Does a supplier safety case remove the need for local clinical safety assessment?

No. Manufacturer evidence supports the buyer's decision, but the deploying organisation must evaluate relevant risks arising from its own users, pathways, integrations, configuration and operating environment. [4][8]

What if the product includes AI or could be a medical device?

Assess the intended purpose and regulatory classification first. For applicable NHS deployments, consider DTAC and clinical risk management alongside medical-device requirements and the specific risks of AI performance, human oversight, change and clinical context. DTAC is not a substitute for medical-device regulation. [1][10]

Which DSPT version should we use in late 2026?

NHS England has published DSPT 2026–27 version 9 evidence items, with the stated submission deadline of 30 June 2027. Requirements differ by organisational category, and relevant assurance or audit arrangements must be checked against the official toolkit. Do not reuse last year's spreadsheet without checking the current version. [5]

Can a third-party adviser certify that a product will pass every NHS assurance gate?

No adviser should imply that a single engagement replaces the accountable buyer's assessment, independent regulatory decisions or the deploying organisation's clinical safety governance. External advisers can help establish scope, review evidence, identify gaps and prepare decision-ready material; the required decisions remain with the appropriate organisations and authorities.

11. How IG-Smart can support the evidence decision

IG-Smart supports organisations needing a defensible approach to information governance, digital health assurance, data protection, cyber governance and the evidence required for procurement and accountable deployment. Depending on the agreed engagement scope, this may include assessing applicable requirements, mapping evidence ownership, identifying gaps, preparing assurance records, supporting clinical safety governance and helping decision-makers understand unresolved risks.

If your NHS digital health purchase, supplier onboarding or procurement response is being delayed by unclear evidence requirements, submit the requirement and relevant context for a scoped discussion with a senior practitioner.

Next step: Submit a Requirement. Alternative where a buyer is exploring an undefined scope: **Talk to a Senior Practitioner.**

Relevant service pathways: [DTAC Readiness](#) · [NHS DSPT Readiness](#) · [Clinical Safety Consultancy](#) · [Clinical Safety Officer Services](#).

Authoritative sources and currency

This guide is based on primary NHS England, NHS DSPT and MHRA publications checked **24 October 2026**. Source descriptions below refer to the public rules; the six-gate evidence chain, scenario matrix and checklist are IG-Smart editorial tools, not statutory tests. Use the current official material when making a procurement or deployment decision.

Scope note: This is not an official NHS assessment or a product-specific clinical safety determination. Check the relevant product, organisation, contract, date and care setting with appropriately competent reviewers.

Sources

- [1] NHS England — Digital Technology Assessment Criteria (DTAC), guidance for buyers and suppliers. <https://digital.nhs.uk/services/digital-technology-assessment-criteria-dtac>
- [2] NHS England - How DTAC works. <https://digital.nhs.uk/services/digital-technology-assessment-criteria-dtac/how-dtac-works> ; Conduct a DTAC assessment. <https://digital.nhs.uk/services/digital-technology-assessment-criteria-dtac/conduct-a-dtac-assessment>
- [3] NHS England — Data Security and Protection Toolkit. <https://www.dsptoolkit.nhs.uk/>
- [4] NHS England — Clinical risk management standards. <https://digital.nhs.uk/services/clinical-safety/clinical-risk-management-standards>
- [5] DSP Toolkit — 2026–27 version 9 category-specific requirements. <https://www.dsptoolkit.nhs.uk/News/169>
- [6] NHS England — National review of DCB0129 and DCB0160. <https://www.engage.england.nhs.uk/patient-safety/national-review-of-clinical-risk-management-standards/>
- [7] NHS England — Applicability of DCB0129 and DCB0160. <https://digital.nhs.uk/services/clinical-safety/applicability-of-dcb-0129-and-dcb-0160>
- [8] NHS England — BaRS clinical safety responsibilities. <https://digital.nhs.uk/services/booking-and-referral-standard/clinical-safety>
- [9] NHS England — Clinical safety documentation. <https://digital.nhs.uk/services/clinical-safety/documentation>
- [10] MHRA — Software and AI as a medical device. <https://www.gov.uk/government/publications/software-and-artificial-intelligence-ai-as-a-medical-device>