CLEARANCE

AI Governance Diagnostic Report

WALES HEALTH

Healthcare · Engagement ref 5a29ed1f-f5f0-4c35-b · 05 August 2026

DEPLOYMENT BLOCKED

Engine v1.6 · Library v1.9.6

CLEARANCE

AI Governance Diagnostic Report

Engagement ref	5a29ed1f-f5f0-4c35-b	**Date issued**	05 August 2026
Organisation	WALES HEALTH	**Engine version**	v1.6 · Library v1.9.6
Sector	Healthcare	**Active layers**	core, gdpr, uk_nhs

DEPLOYMENT BLOCKED: 16 governance gaps identified. 4 Critical · 8 High · 4 Medium

CRITICAL	HIGH	MEDIUM	DEPLOYMENT BLOCKERS
4	8	4	3

This report is the output of a fixed-rules diagnostic evaluation. Every gap was triggered by the intake responses against a fixed gap library. The same inputs produce the same findings every time. This is not a consultant's view. It is a structured result. It does not constitute legal or regulatory advice. Specific regulatory obligations should be confirmed with your legal or compliance adviser.

EXECUTIVE SUMMARY

This assessment of WALES HEALTH's AI deployment identified failures across decision governance and audit capability, data protection and individual rights, and clinical safety and NHS deployment readiness. Individually, these gaps create operational risk. Together, they create a position that would be difficult to defend during an incident investigation, procurement review, or regulatory challenge. This system must not enter or remain in production until the findings below are resolved.

CLEARANCE · AI GOVERNANCE DIAGNOSTIC

Gap Findings

WALES HEALTH · Healthcare · 05 August 2026

Every gap below was triggered by intake signals. Each states when it becomes visible and what closes it. Gaps are ordered by severity.

HIGH

G01-CORE-BOUNDARY

No decision boundary enforcement

An incident investigation asks a simple question: what governed this decision before it executed? For this system, there is no answer. The output became the action with nothing in between.

Regulatory obligations: UK GDPR Art 22C · DUAA 2025 · DCB0160 · EU AI Act Art 9

MEDIUM

G02-CORE-PROVENANCE

Provenance weakness

A regulator or auditor asks where the data came from that drove a specific decision. Tracing it back takes days, not minutes, and for some inputs there is no trail at all.

Regulatory obligations: UK GDPR Art 5(1)(d) · UK GDPR Art 22C · DUAA 2025 · ICO Data Accuracy Guidance

HIGH

G03-CORE-AUDIT

Audit void

A client disputes a decision and asks to see the record. The decision happened. The record of it did not.

Regulatory obligations: UK GDPR Art 22C · DUAA 2025 · DCB0160 · EU AI Act Art 12

HIGH

G04-CORE-ACCOUNTABILITY

Accountability gap

Something goes wrong and the question lands on one desk: who was overseeing this system? The honest answer is no one was, formally, even though someone's name sits next to it.

Regulatory obligations: UK GDPR Art 22C · DUAA 2025 · DCB0160 · EU AI Act Art 14

CRITICAL

G05-CORE-REMEDIATION

Remediation path absent

Investigators do not weigh single gaps in isolation. They look for a pattern with no remediation plan behind it, because that is what separates an organisation that missed something from one that knew and did nothing.

Regulatory obligations: UK GDPR Art 24 · ICO AI and Biometrics Strategy 2025/26 · DCB0160

HIGH

GDPR-G01-LAWFUL-BASIS

No documented lawful basis for AI data processing

An ICO investigation starts with one question: what is the lawful basis for this processing? If the answer was never written down, there is nothing to produce.

Regulatory obligations: UK GDPR Art 6 · UK GDPR Art 9 · DUAA 2025 · ICO Lawful Basis Guidance · Data Protection Act 2018

MEDIUM

GDPR-G02-PURPOSE-LIMITATION

Personal data used by AI beyond its original collection purpose

Someone asks why their data ended up feeding an AI system they never knew existed. The honest answer is that it was collected for something else entirely, and no one checked whether feeding it to this system was still compatible with that original purpose.

Regulatory obligations: UK GDPR Art 5(1)(b) · UK GDPR Art 6 · DUAA 2025 Art 8A · ICO Purpose Limitation Guidance

HIGH

GDPR-G05-VENDOR-DPA

No Data Processing Agreements with AI vendors

A vendor audit, or worse a breach at the vendor, raises an obvious question: what can you compel them to do? Without a DPA in place, the answer is nothing. No deletion right, no processing restriction, no indemnity.

Regulatory obligations: UK GDPR Art 28 · UK GDPR Art 32 · ICO Controller-Processor Guidance · Data Protection Act 2018

CRITICAL

UK-NHS-G01-DCB0160-SAFETY-CASE

Clinical safety case missing

A coroner, or an NHS England safety investigation, asks for the clinical safety case that should have existed before this system was put in front of patients. None exists, because DCB0160 requires one and this deployment skipped it.

CRITICAL

UK-NHS-G02-DCB0160-CSO

No accountable safety owner

After a safety incident, regulators ask one question: who owned clinical risk for this system? No one can give them a name, because DCB0160 requires a named Clinical Safety Officer and none was ever appointed.

CRITICAL

UK-NHS-G03-DCB0160-OVERRIDE

Clinical override missing

The AI produces a recommendation a clinician knows is wrong. There is no tested way for them to stop it reaching the patient before it does.

HIGH

UK-NHS-G04-DSPT

Data security assessment lapsed

NHS Digital flags the DSPT submission as lapsed during a routine data security review. Every other AI governance claim the organisation makes now sits on top of that unresolved gap.

HIGH

UK-NHS-G05-DTAC

Procurement readiness gap

An NHS procurement panel asks for the DTAC assessment before this tool can be formally adopted. Without it, the deployment that already exists is itself procurement non-compliant, and there is no basis to approve scaling it further.

HIGH

UK-NHS-G06-INCIDENT-LOGGING

Incident logging gap

A near-miss involving the AI system happens and nobody logs it, because there is no process that captures AI-related incidents into clinical governance. CQC treats that absence as a missing safety feedback loop, not a one-off oversight.

MEDIUM

UK-NHS-G07-EXPLAINABILITY

Outputs cannot be explained

A clinician is asked to justify a decision the AI influenced and cannot explain the factors behind the system's output. Under CQC and ICO scrutiny, an output that cannot be explained cannot be safely acted on or defended.

MEDIUM

UK-NHS-G08-DCB0129-HAZARD-LOG

Hazard log not maintained

The AI system is updated, retrained or changed, and nobody assesses what new clinical hazards that change introduces. DCB0129 requires a hazard log precisely for this, and none is being kept.

Regulatory Obligations

WALES HEALTH · Healthcare · 05 August 2026

The obligations below are engaged by the gaps identified in this report. GAP: a triggered finding directly engages this obligation. REVIEW: this obligation is relevant to your sector and worth examining. NOT COVERED: this assessment did not include questions for this obligation.

OBLIGATION	RELEVANCE	STATUS
UK GDPR Art 6	Lawful basis must be documented for every AI processing activity involving personal data	GAP
UK GDPR Art 22C	Human review mechanism required for automated decisions affecting individuals	GAP
UK GDPR Art 28	Data Processing Agreements required with every AI vendor processing personal data	GAP
DUAA 2025	AI-specific data rights and oversight obligations under the Data Use and Access Act	REVIEW
DCB0160	Clinical safety case required before deployment of software in clinical settings	REVIEW
NHS DSPT	Data Security and Protection Toolkit, annual submission required	REVIEW
NHS DTAC	Digital Technology Assessment Criteria, required for NHS procurement	REVIEW

NEXT STEP

CLEARANCE identifies gaps. It does not remediate them. Remediation is carried out by a qualified partner. Contact whoever provided this report to discuss next steps.

reports@clearance-diagnostic.com

CLEARANCE · AI GOVERNANCE DIAGNOSTIC

Remediation Roadmap

WALES HEALTH · Healthcare · 05 August 2026

One action per gap. Ordered by timeline. Critical gaps require immediate action. High severity gaps must be addressed within 90 days. Medium severity gaps within 180 days.

TIMELINE	GAP	ACTION REQUIRED	PRIORITY	OWNER
IMMEDIATE	**G05-CORE-REMEDIATION** Remediation path absent	Designate a named individual responsible for AI governance and give them 30 days to produce a written plan. Even a one-page document with milestones is enough to show the organisation is taking this seriously.	CRITICAL	your board
IMMEDIATE	**UK-NHS-G01-DCB0160-SAFETY-CASE** Clinical safety case missing	Appoint a Clinical Safety Officer and initiate the DCB0160 clinical safety case immediately. The system must be removed from clinical pathways until the safety case is completed and signed off.	CRITICAL	your Clinical Safety Officer
IMMEDIATE	**UK-NHS-G02-DCB0160-CSO** No accountable safety owner	Appoint a named CSO with documented clinical safety competence before the next clinical AI decision is made. Record the appointment formally. CQC will treat absence of a named CSO as a systemic accountability failure.	CRITICAL	your Clinical Safety Officer
IMMEDIATE	**UK-NHS-G03-DCB0160-OVERRIDE** Clinical override missing	Design and implement a clinician override mechanism before the system processes another patient record. Every override must be logged with clinician identity, timestamp, and reason. Test the mechanism before returning to production.	CRITICAL	your Clinical Safety Officer
90 DAYS	**G01-CORE-BOUNDARY** No decision boundary enforcement	Introduce a rule evaluation layer between this system's output and the action it takes. Even a minimal documented ruleset is a material improvement on none.	HIGH	your system architect
90 DAYS	**G03-CORE-AUDIT** Audit void	Start logging every decision this system makes today: date, input, output, rule applied, in a write-once store. This is the foundation. Every other governance control depends on it existing.	HIGH	your compliance lead
90 DAYS	**G04-CORE-ACCOUNTABILITY** Accountability gap	Have the accountable individual start an oversight log this week: date, decision reviewed, action taken or confirmed. Even a simple log converts a job title into a defensible position.	HIGH	your compliance lead
90 DAYS	**GDPR-G01-LAWFUL-BASIS** No documented lawful basis for AI data processing	Map every AI processing activity involving personal data to a specific UK GDPR Article 6 lawful basis and record it in a processing register. Complete within 30 days.	HIGH	your Data Protection Officer
90 DAYS	**GDPR-G05-VENDOR-DPA** No Data Processing Agreements with AI vendors	Produce a register of every AI vendor processing personal data on your behalf. Execute DPAs with all of them. Until DPAs are in place, affected tools should not be used with personal data.	HIGH	your Data Protection Officer

TIMELINE	GAP	ACTION REQUIRED	PRIORITY	OWNER
90 DAYS	**UK-NHS-G04-DSPT** Data security assessment lapsed	Complete and submit the current year DSPT assessment. Assign a named DSPT owner. DSPT completion is a procurement prerequisite, without it, NHS contracts are at risk.	HIGH	your Clinical Safety Officer
90 DAYS	**UK-NHS-G05-DTAC** Procurement readiness gap	Initiate a DTAC assessment. Engage the NHSX assessment team or accredited assessor. Without DTAC, the product cannot be formally procured by NHS organisations and any existing deployment is procurement non-compliant.	HIGH	your Clinical Safety Officer
90 DAYS	**UK-NHS-G06-INCIDENT-LOGGING** Incident logging gap	Implement an AI-specific incident and near-miss logging process, integrated with the existing clinical governance framework. Review the log monthly at clinical governance level. Any historic unlogged incidents should be retrospectively recorded.	HIGH	your Clinical Safety Officer
180 DAYS	**G02-CORE-PROVENANCE** Provenance weakness	Create a register of every data source feeding this system. Assign an owner and a validation status to each.	MEDIUM	your system architect
180 DAYS	**GDPR-G02-PURPOSE-LIMITATION** Personal data used by AI beyond its original collection purpose	Identify every AI processing activity using data beyond its original collection purpose. Complete a compatibility assessment for each under DUAA 2025 Article 8A. Update privacy notices before the next data collection cycle.	MEDIUM	your Data Protection Officer
180 DAYS	**UK-NHS-G07-EXPLAINABILITY** Outputs cannot be explained	Define and implement an explainability standard for AI clinical outputs, at minimum, the factors that drove the output and a confidence indicator. Document this in the clinical safety case. Consult the NHS AI Lab explainability guidance.	MEDIUM	your Clinical Safety Officer
180 DAYS	**UK-NHS-G08-DCB0129-HAZARD-LOG** Hazard log not maintained	Initiate and maintain a hazard log under DCB0129. Every material change to the AI system, model update, data change, workflow integration, must be assessed for new clinical hazards before deployment. Assign the hazard log to the CSO.	MEDIUM	your Clinical Safety Officer

CLEARANCE · AI GOVERNANCE DIAGNOSTIC

Evidence Appendix

WALES HEALTH · Healthcare · 05 August 2026

ASSESSMENT RESPONSES

QUESTION	RESPONSE	CATEGORY
AI system is live in production or active pilot	Yes	Your AI system
System makes or influences high-impact decisions	Yes	Your AI system
Decisions execute without individual human review	Yes	Your AI system
A written decision boundary document exists	No	Rules and boundaries
That document is version-controlled and enforced at runtime	No	Rules and boundaries
System uses data from outside the organisation	Yes	Data
Purpose-compatibility assessment completed for external data use	No	Data
Every input is traceable to its origin, owner, and last update	No	Data
Automated validation runs before data reaches the system	Yes	Data
Every decision is logged automatically at the time it happens	No	Records and accountability
A tamper-evident, provable audit trail exists	No	Records and accountability
A functioning human override mechanism exists and is used	No	Records and accountability
A named individual is personally accountable for this system	No	Records and accountability
Documented data subject rights process covers this AI system	Yes	Records and accountability
An incident, near-miss, or complaint has occurred	No	When things go wrong
Documented corrective action was taken following the incident	No	When things go wrong
Does a DCB0160 clinical safety case exist for this AI system?	No	NHS Controls
Is a named Clinical Safety Officer (CSO) designated for this system?	No	NHS Controls
		NHS Controls

QUESTION	RESPONSE	CATEGORY
Is there a mechanism for the CSO to intervene before an AI decision executes?	No	
Has the system been assessed against the NHS DSPT (Data Security and Protection Toolkit)?	No	NHS Controls
Has the system completed the NHS DTAC (Digital Technology Assessment Criteria)?	No	NHS Controls
Is there a sealed incident log covering AI-related near-misses and adverse events?	No	NHS Controls
Can the system explain its outputs in terms a clinician can act on?	No	NHS Controls
Does a DCB0129 hazard log exist identifying risks introduced by this AI system?	No	NHS Controls
Is there a named individual accountable for AI governance in your organisation?	No	NHS Controls

5

NHS Governance Addendum

WALES HEALTH · Healthcare · 05 August 2026

NAMED AI GOVERNANCE LEAD

No named AI governance lead has been identified.

The NHS 10 Year Health Plan and CQC Regulation 12 both require clear accountability for AI systems. A named individual, not a committee or shared job title, must hold documented authority over AI governance policy. This gap increases your exposure in any CQC inspection, board-level audit, or incident review. Appoint and minute a named lead as a priority action.

DSPT CROSS-REFERENCE

The Data Security and Protection Toolkit (DSPT v8) is mandatory for all organisations that access NHS patient data or systems. The table below maps CLEARANCE findings to DSPT evidence requirements. Use this to align your remediation plan with your annual DSPT submission (deadline: 30 June 2026).

Status: DSPT not confirmed for this system. A lapsed or missing submission disqualifies your organisation from accessing NHS systems and may trigger contractual enforcement under the Health and Social Care Act 2012.

CLEARANCE Control	DSPT Standard	Evidence Required
Data governance policy	NDG Standard 1	Named data security lead, documented responsibilities
Staff AI training	NDG Standard 1	Training completion records, awareness programme evidence
Incident logging	NDG Standard 6	AI-related near-miss and adverse event log, sealed and dated
Supplier/vendor controls	NDG Standard 10	AI vendor contracts, data processing agreements
Technical security	NDG Standard 7	Penetration test results, Cyber Essentials certification
Data minimisation	NDG Standard 3	Evidence that AI only processes data necessary for its function

DTAC ALIGNMENT

The Digital Technology Assessment Criteria (DTAC 2026, updated February 2026) is the NHS procurement baseline for all digital health technologies. If your AI system is procured by or deployed within an NHS organisation, DTAC compliance is a threshold requirement.

Status: DTAC not confirmed for this system. Without a completed DTAC, this system cannot be procured by an NHS organisation.

DTAC Area	CLEARANCE Finding	Gap Status
C1 Clinical Safety	DCB0160 safety case; DCB0129 hazard log	See P1, P8 findings above
C2 Data Protection	UK GDPR lawful basis; DSPT alignment; special category data	See data governance findings above
C3 Technical Security	Cyber Essentials; penetration testing; access controls	See technical controls findings above
C4 Interoperability	NHS number validation; FHIR API standards; data format compliance	Verify against your system architecture
C5 Usability and Accessibility	WCAG 2.1 AA; user journey mapping; clinical usability testing	Verify against your deployment evidence

ASSESSMENT INTEGRITY

Organisation: WALES HEALTH
Sector: Healthcare
Run ID: 5a29ed1f-f5f0-4c35-b201-cccf94ded2d2
Engine version: v1.6 · **Library version:** v1.9.6
Active layers: core, gdpr, uk_nhs
Findings hash: 5a29ed1f-f5f0-4c35-b201-cccf94ded2d2
Generated: 2026-08-05T22:04:26.131433+00:00