

A Federated Architecture and Operating Model for National Digital Health at Small-Nation Scale: A Design Blueprint for NHS Wales

Rafal Bergman, PhD

August 2026 — working paper v1.1 · DOI (all versions): [10.5281/zenodo.21445084](https://doi.org/10.5281/zenodo.21445084)

Author affiliation and declaration. Independent researcher; formerly Chief DevOps Officer, subsequently retitled Chief Product and Technology Officer, Digital Health and Care Wales (2024–2025). This paper is the constructive companion to a systems-dynamics diagnosis of the current arrangement (Bergman, 2026a, DOI: [10.5281/zenodo.21444618](https://doi.org/10.5281/zenodo.21444618)); it can be read independently. Every component proposed here is in operational use in a comparator jurisdiction; the design's claim to validity rests on that constraint, not on the author's positionality. Correspondence: rafal@ctozen.com. The full blueprint, with sources for every figure, is published open-access as part of the *Digital Blueprint for NHS Wales* at <https://bluenhs.org/blueprint/> (CC BY 4.0).

Version note. v1.1 (August 2026) aligns the paper with the expanded evidence base of the incumbent's documented failure — now published as a numbered, archived source register, *The State of DHCW* (86 numbered references, 48 archived public-sector documents), at <https://bluenhs.org/state-of-dhcw/> — and cites the companion diagnosis by its version-independent DOI. Two schematic figures added. The design, costings and conclusions are unchanged from v1.0.

Abstract

Small nations repeatedly attempt national digital health through a single delivery body that builds, buys and runs everything — and repeatedly fail. This paper presents the alternative as a specified design rather than a policy aspiration: a federated architecture and operating model for a 3.1-million-person health system, developed for NHS Wales and generalisable to jurisdictions of comparable scale. The design applies one constraint throughout: no component is proposed unless it already operates at scale in a comparator jurisdiction — Denmark's standards-body pattern (MedCom, Sundhedsdatastyrelsen), Estonia's federated exchange (X-Road, TEHIK), or NHS England's externally-recruited delivery leadership. The architecture comprises six independently procurable layers under five design principles, the central two being the separation of standards from delivery and federation of the patient record as a query across the systems that hold the data, rather than a monolithic national platform. The operating model specifies a standards-and-interoperability body of roughly 400 staff at £45–60M per year — against the current 1,263-staff, ~£200M monopoly — with a named destination for every current post, a 36-month strangler-fig transition costed at £5–15M, and a first-90-days sequence. A striking property of the adoption path is that almost none of it requires primary legislation: the monopoly was made by executive instruments and can be unmade by them. The

design states its own falsification criteria: six published tests for the ten-year digital programme the Welsh Government has announced, and a monitoring baseline whose 12- and 36-month targets the reform must meet. The contribution is a worked, costed, testable existence proof that small-nation digital health does not require a monopoly — and a template for the class of jurisdictions between one and six million people facing the same choice.

Keywords: digital health; enterprise architecture; interoperability; federation; operating model; NHS Wales; public-sector reform; standards bodies

1. Introduction

The diagnostic literature on national health IT failure is rich; the design literature is thin. Post-mortems of England’s National Programme for IT, Denmark’s Sundhedsplatformen go-live and comparable cases identify what went wrong, but jurisdictions facing the design decision — *what should the national digital function actually be?* — find few worked answers at their scale. The gap matters most for small nations: large jurisdictions can absorb a failed platform programme; a 3.1-million-person system cannot.

This paper presents such a worked answer, developed for Wales. The companion paper (Bergman, 2026a) establishes why the incumbent arrangement — a statutory monopoly that fuses standards-setting with application delivery — fails structurally rather than managerially: eleven reinforcing feedback loops, all seven of Meadows’ system traps simultaneously active, and failure conditions co-authored by the funder. That diagnosis implies a design brief with three requirements: separate standards from delivery; federate rather than centralise the record; and reform the funding regime in parallel. This paper is the response to that brief, but it stands alone: the design is justified component-by-component from international precedent, not from the Welsh pathology.

The design is published in full, with diagrams, costings and per-claim sources, at <https://bluenhs.org/blueprint/>; this paper is its academic statement.

2. Method: precedent-constrained design

The design method applies a single admissibility rule: **no component may be proposed unless it is in operational use, at scale, in a jurisdiction comparable to or smaller than Wales.** The rule is deliberately conservative. It excludes novelty — including several components the author would otherwise favour — and it converts the design argument from speculation (“this should work”) to selection (“this works; here is why this combination fits Wales”).

Three reference architectures supply the components:

- **Denmark** (5.9M, five regions): a national standards body (Sundhedsdatastyrelsen) and a non-profit interoperability certifier (MedCom, est. 1994) sit above regions that procure their own EHRs. The national patient portal sundhed.dk (2003) is built on MedCom’s

infrastructure. Standards are separated from delivery; regions have real procurement power.

- **Estonia (1.3M):** the X-Road federated data-exchange layer (2001, open source, now co-developed with Finland through the Nordic Institute for Interoperability Solutions) connects every EHR; no single body holds the clinical data. TEHIK, the national health IT authority, runs the connective tissue for 1.3 million people with roughly 200 staff. The national e-health record is a virtual record assembled at query time.
- **NHS England:** central standards, competitive national services, trust-level procurement — and, decisively, executive technology leadership recruited from the open market against published criteria.

The three differ in detail and share a structure: a thin national body owns interoperability; providers own applications; leadership is recruited, not inherited. The incumbent Welsh model inverts all three commitments. The design below is the Welsh translation of the shared structure.

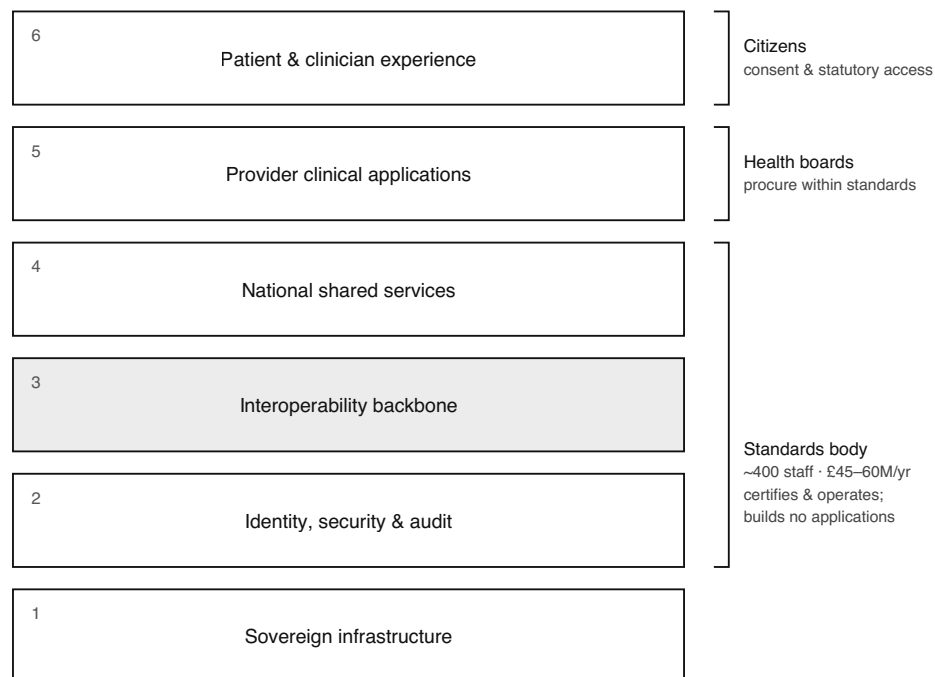
Validity is addressed a second way: the design publishes its own falsification criteria (Section 7). A design that specifies measurable success conditions in advance can be wrong in public — which is the property that distinguishes a blueprint from an aspiration.

3. Five design principles

1. **Standards are separated from delivery.** A small national body sets and certifies interoperability standards and builds no clinical applications; health boards procure applications within those standards. This is the load-bearing principle: it removes the structural conflict of a standards-setter judging its own delivery.
2. **Federation, not centralisation.** Patient data lives in the system that generated it; a national interoperability backbone makes the federation queryable. The record looks unified; no monolithic database exists; no single supplier outage can take the estate offline.
3. **Open standards by default.** HL7 FHIR R4, SNOMED CT, dm+d, ICD-10/11, OpenID Connect, OAuth 2.1, IHE profiles, X-Road or equivalent. Welsh requirements (statutory bilingualism, devolved policy) are extensions of international standards, never replacements. Conformance is a technical gate in procurement, not a policy preference.
4. **Open source for shared infrastructure.** The backbone, terminology services, audit ledger, identity broker and citizen app are open source by default: sovereign, inspectable, forkable. Estonia and Finland share X-Road on exactly this basis; the pattern is available to any small nation as member or fast-follower.
5. **Building blocks, not platforms.** Every national component does one thing and exposes a typed API. The international failure cases (NPfIT, Care.data) were platforms; the successes (X-Road, sundhed.dk, GP Connect) are building blocks. Platforms become unkillable because everything depends on the whole; building blocks stay replaceable because consumers depend on contracts.

4. The reference architecture

The architecture has six independently procurable, testable and replaceable layers.



automated public conformance testing at every layer boundary; no component owned by more than one principal

Figure 1. The six-layer reference architecture and its three principals. The standards body certifies and operates layers 2–4 and builds no clinical applications; health boards procure layer-5 applications within published standards; citizens hold consent and statutory access rights at layer 6. The interoperability backbone (layer 3, shaded) is the thinnest and most load-bearing layer.

Layer 1 — Sovereign infrastructure. UK-resident cloud with sovereign zones, high-availability networking with statutory (not discretionary) redundancy, national DNS authority, public-sector certificate authority, cyber-defence operations. The redundancy requirement is a direct lesson of the Welsh record: three consecutive years of single-dependency infrastructure failure, culminating in a 2026 network outage that took every NHS Wales organisation offline simultaneously.

Layer 2 — Identity, security, audit. National citizen identity (OpenID Connect, federable with UK-wide services), national clinician identity (FIDO2/passkeys), an immutable append-only audit ledger every layer writes to and none can rewrite, and a national PKI. Security operations are structurally separate from delivery.

Layer 3 — The interoperability backbone. An X-Road-equivalent federated exchange; a FHIR API gateway handling routing, versioning, conformance and rate-limiting; a clinical-event bus (admission, discharge, transfer, prescription, referral); national terminology services exposed as APIs. This is the thinnest and most load-bearing layer, and the strongest candidate for direct adoption of existing open-source stacks rather than bespoke national code.

Layer 4 — National shared services. The small set of services that genuinely benefit from national operation: demographics (the national patient index), practitioner index, electronic prescription gateway, referral and booking gateway, a **federated national care record assembled at query time from source systems**, and a population-health data platform for analytics and research. Each is a building block with a typed FHIR API; none holds the clinical record.

Layer 5 — Provider clinical applications. EPRs and clinical systems procured by health boards within the national standards. Conformance with layers 2–4 is the gating criterion; the brand of EPR is a provider decision. Boards may procure jointly by choice, never by mandate.

Layer 6 — Patient and clinician experience. The citizen app (statutory bilingual parity, accessibility-first, with an assisted non-digital route for every service), a granular consent surface, a clinician workspace aggregating views across systems, and a public dashboard publishing waiting times, performance and incidents at statutory frequency.

Responsibility is distributed among three principals — the standards body (layers 2–4), health boards (layer 5), citizens (consent and access at layer 6) — with **no component owned by more than one principal**, and automated public conformance testing at every boundary. Clinical applications must pass the standards body’s conformance suite; national services must pass a citizen-rights conformance suite ratified by a statutory patient council. The behavioural difference from the monopoly is structural: under federation, the failure of any single node is local; under monopoly, every failure cascades through the centre.

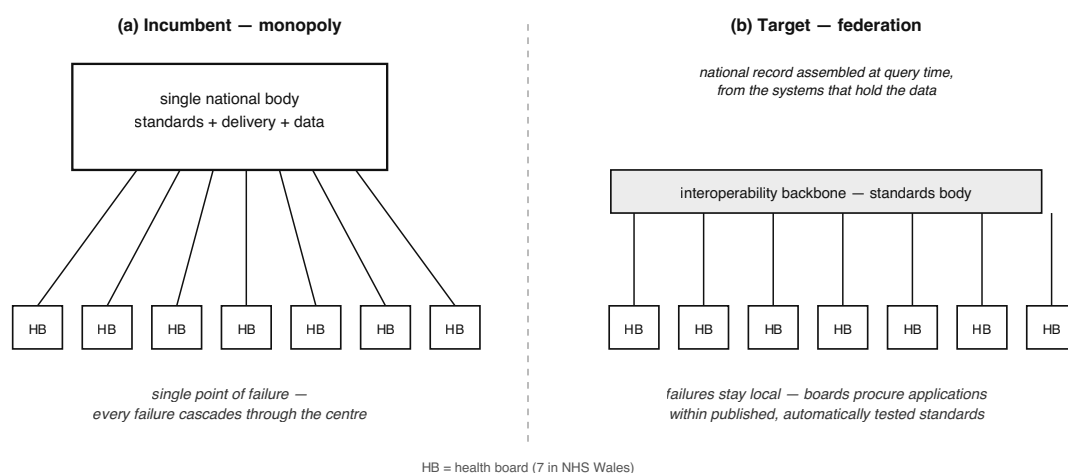


Figure 2. The structural difference between the incumbent and target arrangements. (a) Under monopoly, standards, delivery and data are fused in one body and every health board depends on the centre. (b) Under federation, a thin backbone makes provider-held data queryable; the national record is assembled at query time and single-node failures remain local.

5. The operating model

The architecture requires an organisation of a specific, bounded shape. Scaled from TEHIK (200 staff per 1.3M population), the Welsh standards body runs at **roughly 400 staff and £45–60M per year** at steady state — against the incumbent’s ~1,300 staff and ~£200M. It performs

six functions and nothing else: standards and conformance; platform operations (run as products with published SLOs); the national shared services; cyber defence; architecture and assurance, including post-mortems published within 14 days; and enablement of provider digital teams — advising, never mandating product choices.

Three structural rules hold the shape: every function publishes a service catalogue and unit cost; corporate services never exceed 10% of headcount; and **the body has no programme-delivery directorate** — the moment it acquires one, the monopoly is rebuilding itself. The executive team of six is recruited externally, at market rates, against published technical criteria, by an external panel — the NHS England recruitment pattern, which the comparator evidence treats as mechanism rather than correlation: the recruitment process determines the delivery outcome.

The politically decisive question — what happens to the incumbent’s 1,263 staff — is answered by design rather than left to attrition: approximately 400 map to the standards body’s functions; 300–450 transfer with their work into embedded delivery teams in health boards under protected staff-transfer rules; the remainder — largely programme and corporate roles that end with the monopoly — are handled through funded retraining, redeployment across the wider system and natural attrition over the transition, not a cliff-edge redundancy round. The funding differential (~£140–155M per year) does not leave the health system: it moves to providers as delivery funding for the application layer, under multi-year programme envelopes released at externally assessed gates — the funder-side reform the companion paper shows to be a precondition rather than an accessory.

6. Transition and adoption

The migration is a 36-month strangler-fig, not a rip-and-replace. Existing systems remain in operation; new capability is built behind the national API gateway; legacy systems are retired one at a time once replacements are demonstrably stable in clinical use. Day one establishes a public continuity register: every national service in clinical use, each with a named accountable owner, a runbook, and a designated destination (standards body, health board, or retirement); no service changes hands without its runbook and a shadow-running period. People move with their services, never ahead of them. The transition is costed at £5–15M one-off — against a documented direct waste rate of £100–150M per year in the incumbent arrangement, a break-even measured in weeks.

The adoption path has an underappreciated property: **almost none of it requires primary legislation**. The incumbent monopoly was constituted by executive instruments — establishment orders, remit letters, appointment powers — and every structural move (leadership reset, re-scoping to a standards body, multi-year funding envelopes) can be made by the same instruments. Statute is required only where discretion must be permanently removed: the publication duties (board minutes at transcript fidelity, contracts above threshold, workforce statistics) that make the reformed arrangement inspectable. A first-90-days sequence — live public status page for clinical systems, transcript-fidelity minutes, published contract register, a

named independent digital expert, and one clinician-chosen visible fix per health board — buys the political time a 36-month reform needs.

7. Evaluation: how this design can fail in public

A design proposition is only as credible as its falsification criteria. This one publishes two sets.

First, **six tests for the announced programme**. The Welsh Government has committed to a ten-year digitisation programme including “a road map of a single integrated patient record”. The design predicts the programme succeeds only if: the record is federated rather than platform-built; standards are separated from delivery; funding is multi-year and gate-released; leadership is externally recruited against technical criteria; transparency is statutory; and the funder’s own decision-making is inside the reform scope. The tests were published before the programme’s announcement (<https://bluenhs.org/ten-year-digital-programme/>) precisely so the announcement can be scored against them.

Second, **a monitoring baseline with dated targets**. The blueprint specifies 12- and 36-month targets — delivery, interoperability conformance, workforce, transparency — against a published baseline. If a reform on this design misses them, the design is wrong in a specific, identifiable way; if a reform on the incumbent design meets them, the diagnosis was wrong. Both outcomes are informative; neither is deniable.

8. Generalisability

The design travels. The class of jurisdictions between roughly one and six million people — small EU states, devolved UK nations, Canadian provinces, New Zealand — faces the same structural choice between monopoly delivery and federated standards, usually with the same asymmetry: the monopoly is easier to announce, the federation is easier to run. Three portable results: (i) the connective tissue for a small nation is a bounded, specifiable organisation of a few hundred people, not a thousand-person delivery body; (ii) the admissibility rule — nothing without an operating precedent — converts architecture debates from taste to evidence; (iii) the adoption analysis should begin with what existing executive instruments can do, because the answer is usually “almost everything”, and the belief that reform requires legislation is itself a source of delay.

Limitations. This is a design proposition grounded in comparator evidence and one jurisdiction’s documented failure, not an evaluated implementation; the costings are planning figures anchored to published comparator budgets; and the comparators’ success has institutional preconditions — notably sustained cross-party consent in Denmark and Estonia — that a design document can specify but not supply. The strongest available mitigation is Section 7: the design will be tested in public, on a known timeline, against criteria published in advance.

9. Conclusion

Small-nation digital health does not require a monopoly. Denmark, Estonia and England demonstrate the components; this paper assembles them into a complete, costed, adoptable

design for Wales: six layers, five principles, a 400-person standards body, a federated record, a 36-month transition, and an adoption path that fits inside existing executive powers. The design's distinguishing commitment is falsifiability — six published tests and a dated monitoring baseline — because the difference between a blueprint and an aspiration is that a blueprint can be wrong in public. Wales, having announced the reviews and the ten-year programme that will decide the question, is now the natural experiment.

References

- Bergman, R. (2026a). *Structural Failure in National Health IT: A Systems-Dynamics Case Study of Digital Health and Care Wales*. Working paper. <https://doi.org/10.5281/zenodo.21444618>
- Bergman, R. (2026b). *Digital Blueprint for NHS Wales*. <https://bluenhs.org/> (CC BY 4.0). [Full design, diagrams, costings and per-claim sources.]
- Bergman, R. (2026c). *The State of DHCW: The Documented Record, 2018–2026*. <https://bluenhs.org/state-of-dhcw/> [86 numbered primary sources; 48 archived public-sector documents.]
- Danish Health Data Authority (Sundhedsdatastyrelsen). <https://sundhedsdatastyrelsen.dk/>
- e-Estonia. *X-Road interoperability services*. <https://e-estonia.com/solutions/interoperability-services/x-road/>
- MedCom. *The Danish healthcare data network*. <https://medcom.dk/>
- Meadows, D.H. (2008). *Thinking in Systems: A Primer*. Chelsea Green.
- National Audit Office (2011). *The National Programme for IT in the NHS: an update*. HC 888.
- Nordic Institute for Interoperability Solutions (NIIS). <https://niis.org/>
- Senedd Cymru, Public Accounts Committee (2018). *Informatics Systems in NHS Wales*. CR-LD11822.
- TEHIK — Health and Welfare Information Systems Centre. <https://www.tehik.ee/en>
- Welsh Government (2026). Record of Proceedings, Plenary, 14 July 2026. <https://record.senedd.wales/Plenary/16085>