PDHC — Planned Data in Healthcare

Platform brief

2026-08-13

1. What PDHC is

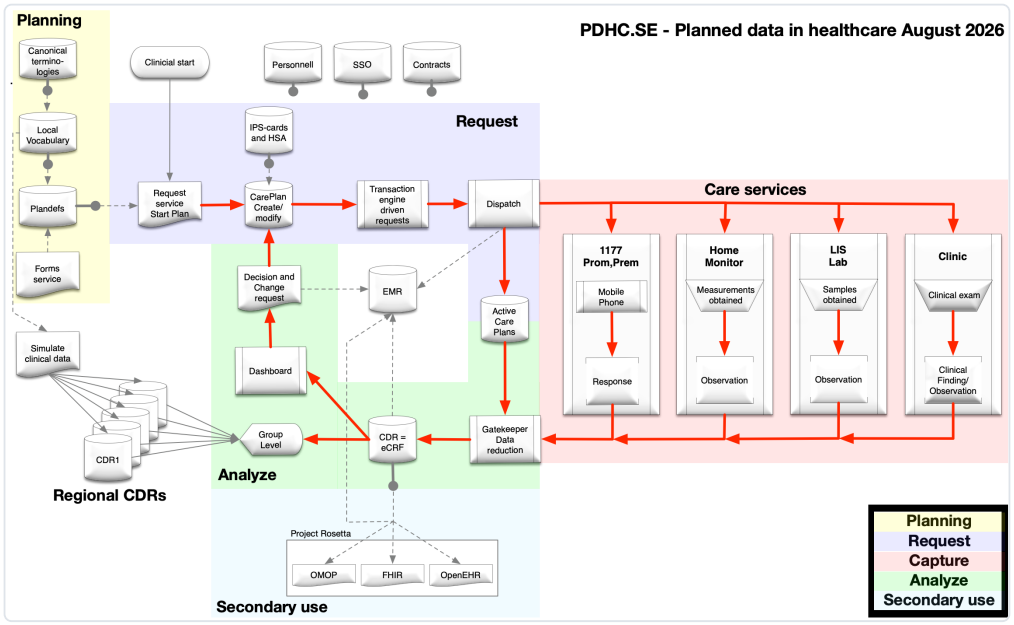
PDHC (Planned Data in Healthcare, `pdhc.se`) is a platform for **planned, structured clinical data capture**: care is described up front as a machine-readable *plan*, that plan is turned into concrete *requests* for data, the requests are dispatched to the party best placed to answer them (a clinic, a device vendor, a remote-monitoring provider, or the patient), and the answers flow back as governed, consented, standards-based observations that downstream analysis can trust.

The design goal is that **every data point has provenance**: which plan asked for it, under which contract, for which patient, from which provider, with which consent — recorded on the observation itself rather than inferred later. PDHC is built on **FHIR R5** and interoperates outward to **openEHR** and **OMOP**.

It is realised as roughly **twenty independent microservices**, each with its own database, deployment, and bounded responsibility, composed into one pipeline. Internal references are **GUID-only** across service boundaries, so services stay decoupled and no integer identity ever leaks between them.

2. Architecture at a glance

The platform is a pipeline from *intent* through governed capture to analysis and secondary use:



*PDHC platform architecture (pdhc.se). **Planning** authors canonical terminologies and PlanDefinitions; **Request** starts the plan, builds/modifies care plans, drives transaction requests and dispatches them; **care providers** (1177, home monitoring, lab, clinic) capture responses and observations; the **Gatekeeper** reduces captured data into the CDR (the eCRF); **Analyze** monitors and can raise change requests; **Regional CDRs** and **Project Rosetta** (OMOP / FHIR / openEHR) serve secondary use.*

Service	Responsibility
sso	Identity, roles, affiliations; access blob rebuilt per-login from affiliations (no stale cache)
plan	Clinical concepts, PlanDefinitions, FHIR R5 terminology (ValueSet/CodeSystem/ConceptMap), AI-assisted authoring
contract	Data-sharing agreements between requesting orgs and providers; the scope a dispatch is matched against
request	Builds ServiceRequests from plans, matches eligible providers, dispatches (push or poll), issues grants/PATs
ips	Patient registry, clinic assignment, **spärr** (blocking) and consent predicates
gateway	Authenticated provider ingest; stamps concept/unit/ranges from request context; forwards to CDR
cdr1–5	Clinical Data Repositories (the analysis record); **cdr_6** is the simulation sink
dashboard / analyse	Single-patient clinical view and the consent-gated analysis engine
rosetta	Interoperability: openEHR (templates + delivery) and OMOP export
provider1 / cgm / 1177	Reference provider portals (remote-monitoring, CGM devices, patient 1177 forms)
sim	Synthetic longitudinal data from real PlanDefinitions (incl. Synthea import) for testing at scale

Each service runs behind a shared reverse proxy on `*.pdhc.se`, binds only to loopback, and validates every request against SSO live (no cached authorisation), so a logout or a consent change takes effect immediately across the platform.

3. Capabilities delivered

Authoring & terminology. Clinicians author concepts and PlanDefinitions in `plan`, with a live FHIR R5 terminology profile (`$expand`, `$validate-code`, `$lookup`, `$translate`). An **opt-in, guarded AI-assisted PlanDef builder** pairs deterministic validators with a selectable-model assistant that never touches the save path.

Contracts, requests & dispatch. `contract` records who may exchange what with whom. `request` turns an active plan into a ServiceRequest, finds the providers eligible under a matching contract, and **dispatches** — either by pushing the FHIR bundle to the provider's inbox or by letting the provider poll a subscription feed. Each dispatch issues a scoped, revocable **Provider Access Token** and a per-exchange **grant**.

Provider ingest & the clinical record. Providers report through `gateway`, which authenticates them, resolves the authoritative concept/unit/response-type from plan context, and forwards a canonical observation to **cdr1**, the clinical record that `dashboard` and the analysis services read. Reference portals (**Provider1**, **CGM**, **1177**) implement the full task-to-report loop (accept, observe, receipt) and serve as the integration template for external partners.

Interoperability. `rosetta` renders and delivers **openEHR** (templates synthesised from PlanDefinitions; FLAT ingest; AQL round-trip) and exports **OMOP**, so PDHC data is portable to external CDRs and research warehouses.

Simulation. `sim` generates realistic longitudinal cohorts from real PlanDefinition terms (and imports **Synthea** populations), lands them in `cdr_6`, and can transfer them into any analysis CDR — enabling end-to-end testing at population scale without touching real patients.

4. Security, consent & legal considerations

PDHC operates under three overlapping legal regimes — **GDPR**, the Swedish **Patient Data Act (Patientdatalagen, PDL)** together with **Lag (2022:913)** on cross-caregiver records, and the **Medical Device Regulation (MDR)**. Its security controls are designed to map onto specific obligations in each; the walkthrough below pairs every legal provision with the control that answers it.

GDPR — lawful basis, purpose limitation, minimisation. Because the data is *planned* — every observation is bound to the concept a PlanDefinition asked for, under a named contract — purpose limitation and data minimisation are **structural rather than retrospective**: the platform only ever requests the data a care plan justifies. Special-category (health) processing rests on the care-provision basis and, for secondary use, on explicit-consent / EHDS bases; **EHDS opt-out and research consent are enforced at query time** in the analysis services, and every access is logged (accountability, Art. 5(2)). Authorisation is rebuilt per-login and never cached, so a withdrawal takes effect immediately across the platform.

PDL & Lag (2022:913) — block, consent, logging, acting-as. Swedish patient-data law is met by four built controls, each closing a specific provision:

- **Spärr (patient block)** — the *inre* / *yttre* / *nödöppning* zone model (PDL Ch. 4 §§ 4–5; Lag 2022:913 § 5, block side). Cross-service checks are relationship-free and **fail closed**; break-glass is granted and audited.
- **Patient consent** — enforced on the contract/dispatch and analysis-read surfaces (Lag 2022:913 § 5, consent side).
- **Read-side audit + correlation** — every read is logged and correlatable by session across services (PDL Ch. 4 § 3; cross-caregiver logging).
- **Acting-as model** — the SSO reform's *vårdgivare* / *vårdenhet* affiliations with per-affiliation roles (PDL Ch. 4 § 2) fix the purpose each read runs under; non-admins see only their own organisation's data.

MDR — qualification, classification, intended purpose. The governing control is the **intended-purpose statement**: it decides qualification and class, and therefore the entire compliance burden. On the current draft:

- The component that **applies thresholds and raises data-driven alerts** (today `request.pdhc`) most likely **qualifies as medical device software** and classifies **Class IIa under MDR Rule 11** — it informs a therapeutic / monitoring decision with a clinician in the loop.
- Components that only **author/store plans** (`plan.pdhc`) or **store, transport or display** data are arguable as **not a device** or **Class I**, *provided the intended purpose is drawn tightly*.
- The **IIa-vs-IIb** line must be backed by an **ISO 14971 risk analysis**: if a missed or late alert could plausibly cause serious deterioration before a clinician acts, a Notified Body may push to IIb — so IIa is **not** asserted by default. Class IIa **requires a Notified Body** (budget 12–24 months and a standing QMS).

Residual legal actions (tracked): sign off the qualification & classification rationale; complete the ISO 14971 / clinical-evaluation evidence for the alerting component; and close the PDL roadmap's remaining authorisation-hardening items. These are organisational commitments, not documentation afterthoughts. *(Sources on disk: `css_instrux/pdhc_mdr_class_iia_classification`, `analysis/pdl_compliance_roadmap`, and the GDPR/MDR cross-section drafts under `docs/upphandling/`.)*

5. Scalability & data independence

PDHC's microservice design is a **scalability strategy**, not merely a way of organising code. Three principles let the platform scale from a single consolidated host to a distributed, multi-tenant deployment without rewrites.

Separable services — scale by moving, not refactoring. Every service owns its database, its container, and its configuration; communicates only over HTTP; and references other services purely by **GUID** — never a shared table or an integer foreign key. Each binds to loopback behind the shared reverse proxy and re-validates authorisation against SSO on every request, so nothing depends on co-location or a shared session store. Running consolidated on one host today is a packaging choice, not an architectural limit: a hot service — `gateway`, a CDR, `request` — can be lifted onto its own server, or replicated behind a load balancer, by changing a base URL and a DNS record. Stateless worker processes scale horizontally within a host; shared-nothing databases scale independently per service.

Self-contained data, free of application dependence. Data is stored in a **self-describing** form that carries its own meaning. Every observation records, on the row itself, its concept (as an embedded GUID, e.g. `urn:pdhc:concept/<guid>`), its unit, and its full provenance — plan, contract, requesting org, provider, patient, and service-request. Clinical records are standards-based **FHIR R5** resources. The consequence is that the data does **not** need the application that produced it in order to remain interpretable: it can be exported, migrated, backed up, or read by a different system and still be understood. The application is a lens over the data, never a prerequisite for it.

Federated CDRs. The clinical record is not one monolith but a set of independent repositories (**cdr1–5**, plus the `cdr_6` simulation sink). The analysis layer **federates** across them — a single query spans multiple CDRs without centralising their storage — and new CDRs can be added, partitioned by region, tenant, or care-giver, and joined for analysis on demand. Data moves between CDRs over cursor-paginated export/transfer paths, and outward to external repositories via **openEHR** and

OMOP. Federation lets the record grow horizontally and cross organisational boundaries while consent and spärr continue to gate every read.

6. Open source & transparency

PDHC is built as an **open-source reference implementation** of planned, consented, standards-based health-data exchange. The reasoning is that a platform governing sensitive patient data earns trust by being **inspectable**: a customer, auditor, or regulator can read exactly how spärr, consent, the MDR scope boundary, and per-observation provenance are enforced, rather than taking a vendor's word for it. Openness also serves adoption — the reference provider portals double as an integration template a partner can read and copy — and avoids lock-in for the healthcare organisations that deploy it.

The **majority of the service repositories are public** on GitHub, with a deliberate few kept private where publishing adds risk without benefit (the synthetic-data simulator, server/operations tooling, and internal regulatory instruments) and a handful of internal utilities that remain local-only. Credential hygiene is a **release gate**: `.env` files are never committed, and a repository's history is scrubbed of any historical secret — at both blob and commit-message level — *before* any private-to-public flip.

The intent is not merely to publish code but to offer a **working, auditable blueprint** for how planned data in healthcare can be requested, governed, and analysed under GDPR, PDL, and MDR — one that others can run, verify, and extend.

7. Current status & near-term

Live today: the full intent-to-analysis pipeline (ingest, record, analysis); SSO reform; spärr zone model and analysis consent enforcement; plan.pdhc FHIR terminology; gateway-to-cdr1 forwarding; openEHR/OMOP export via rosetta; sim + Synthea; reference provider portals.

In flight:

- **External partner onboarding (Medituner AB)** — asthma/COPD remote monitoring; credentials issued, awaiting partner receiver + first sandbox dispatch. (Distinct from the internal *Provider1* reference portal, whose identity was recently disambiguated to remove naming collision.)
- **openEHR delivery** consolidation on rosetta against an external sandbox CDR.
- **AI PlanDef authoring assistant** — general-availability UI and fail-closed operator sign-off.
- Ongoing per-service **run-through** verifying each service against real end-user examples and closing findings as they surface.

PDHC platform brief — generated 2026-08-13. Source of truth is the running code and each service's `progress.md`; this brief summarises, it does not supersede them.