India Consumer Health Data Aggregator

Architecture Diagrams and MVP Wireframes · Companion to Report v1.1 · 21 October 2026

Contents	Part A: Architecture diagrams (Fig 1–8, Mermaid) · Part B: MVP wireframes (W01–W12, low fidelity)
Sources	Mermaid sources (`.mmd`), SVG and PNG renders, and the HTML wireframe board are included in the deliverables ZIP. Diagrams can be edited and re-rendered with `mmdc`.
Status	Design artefacts for discussion. ABDM/NHCX technical details follow NHA's public repositories; regulatory items carry the same validation caveats as the main report (Appendix B).

Part A — Architecture diagrams

Nine diagrams: ecosystem context, logical architecture, ABDM consent and data flow, document AI pipeline, consent lifecycle, the two-part Health Graph data model, security zones, and the capability roadmap. Each page gives the figure, what it shows, and the report sections it supports.

Fig 1 — Ecosystem context

Where the aggregator sits. ABHA provides identity and addressability, not storage. The HIE-CM and Gateway carry consent and routing. HIPs push encrypted FHIR R4 bundles directly to the aggregator. Direct channels (devices, documents, manual entry) sit outside ABDM. NHCX is participant-only (PAYER/PROVIDER/TPA, verified from NHA's repository), so insurance data reaches the consumer app via documents and partnerships. Report refs: §3.1, §3.4, §5.1.

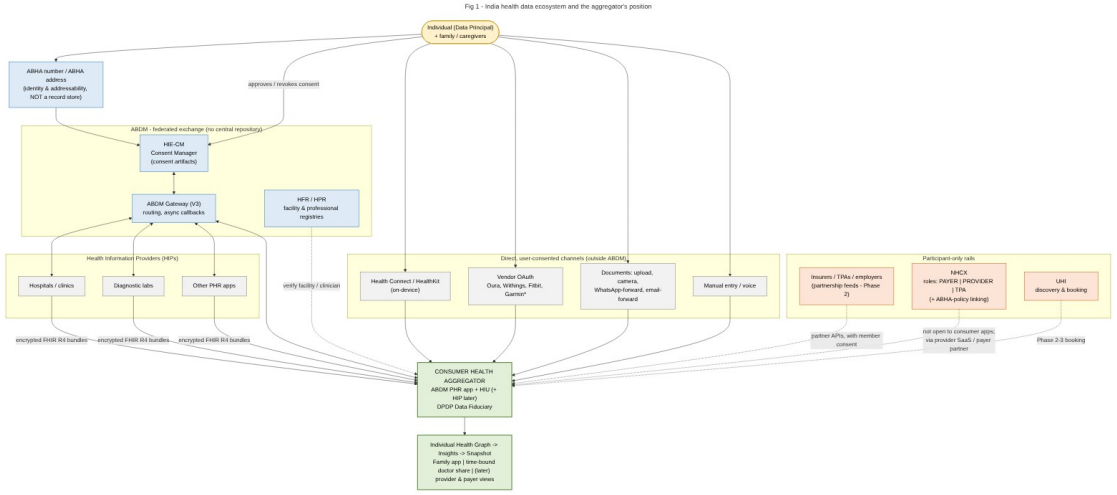


Fig 2 — Logical architecture (layered)

Six layers: channels, edge and policy enforcement (every call passes the ABAC Policy Decision Point), acquisition services, normalisation (FHIR ⇄ graph with provenance and trust tier), intelligence and experience services, and the data plane in an India region with per-person keys. External dependencies are limited to ABDM, an India-region OCR vendor, licensed terminology and an India-hosted LLM behind the AI Gateway. Report refs: §10.1, §10.5.

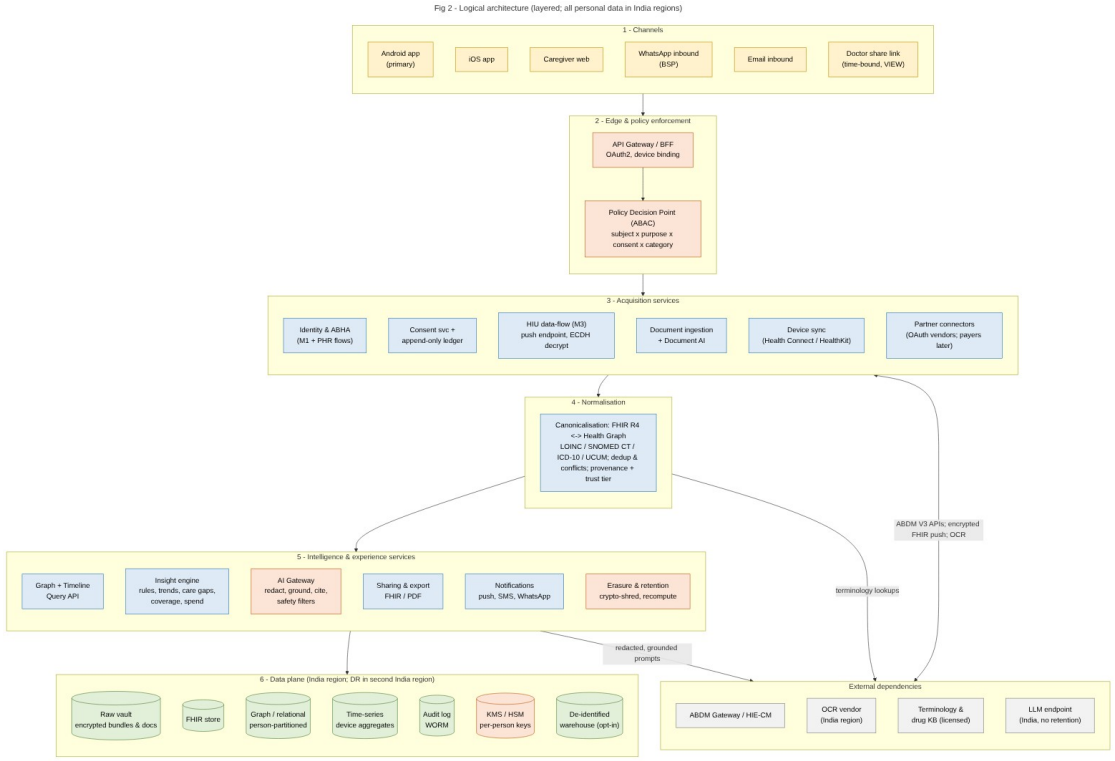


Fig 3 — ABDM self-access consent and data flow

Corrected asynchronous sequence: discovery and linking, consent request with permission (accessMode, dateRange, dataEraseAt, frequency), approval in the PHR/ABHA app, consent-notify callback, artefact fetch, health-information request with a fresh X25519 key pair, encrypted push to the data-push URL, ECDH→HKDF→AES-GCM decryption, NRCES validation, canonicalisation and transfer notification. The alternate path shows revocation/expiry handling. Report refs: §5.2, §10.2, §10.3.

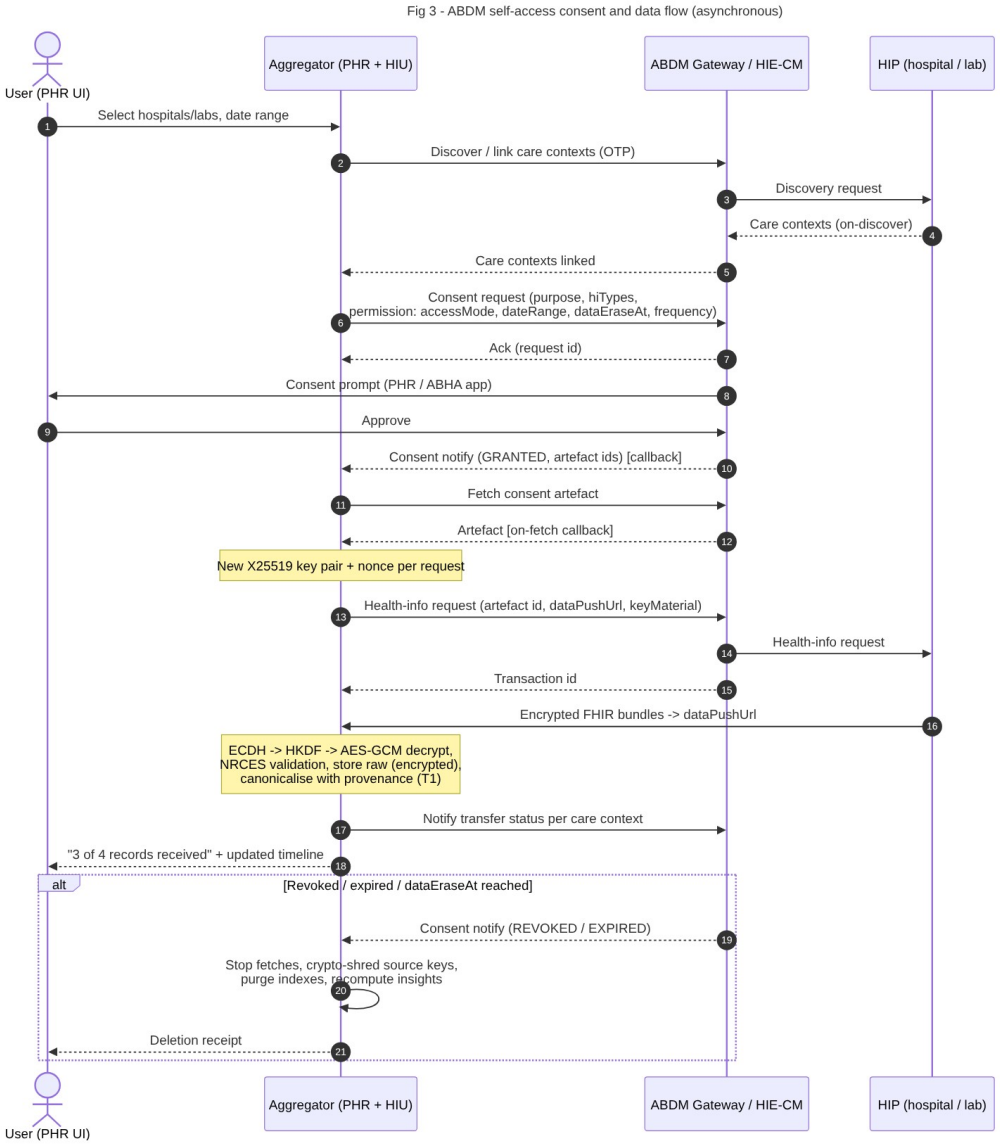


Fig 4 — Document AI pipeline

Intake from upload, camera, WhatsApp, email and share sheet; pre-processing; OCR; classification; a person-match check for shared family phones; extraction and normalisation to LOINC/SNOMED/ICD/UCUM and brand→molecule; confidence routing. Handwritten drug lines always require confirmation; skipped values are held and excluded from insights. Report refs: §6.5, §10.4.

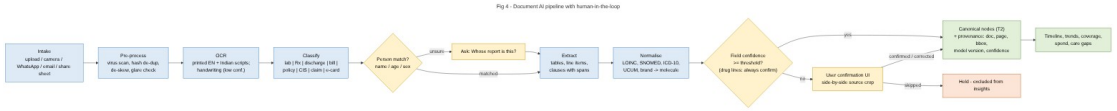


Fig 5 — Consent lifecycle

A single state model for ABDM artefacts and platform purposes. Withdrawal or expiry (including dataEraseAt) triggers erasure: crypto-shredding of source keys, index purge, insight recomputation and a deletion receipt. Legal-hold items are minimal and disclosed. Report refs: §5.4, §7.9.

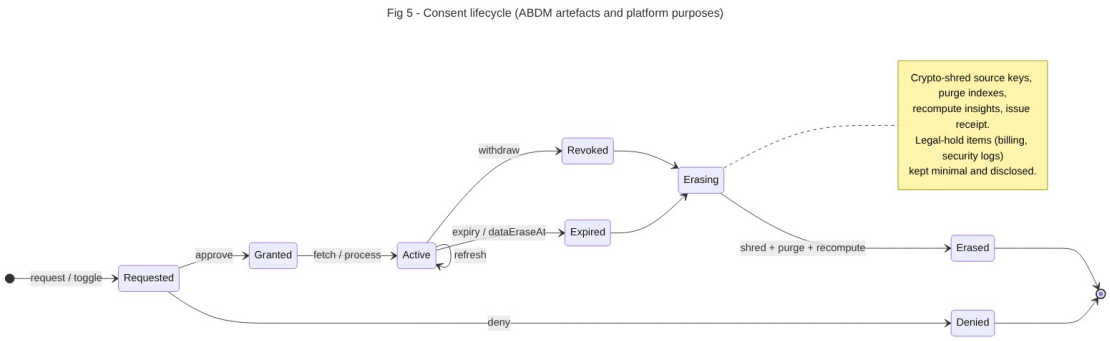


Fig 6a — Health Graph: identity, family and clinical entities

Core clinical entities and relationships. Every node also carries the common provenance envelope (source, raw reference, consent IDs, ABDM transaction, extraction confidence, verification status, retention), not drawn here for readability. Report refs: §6.2–6.4.

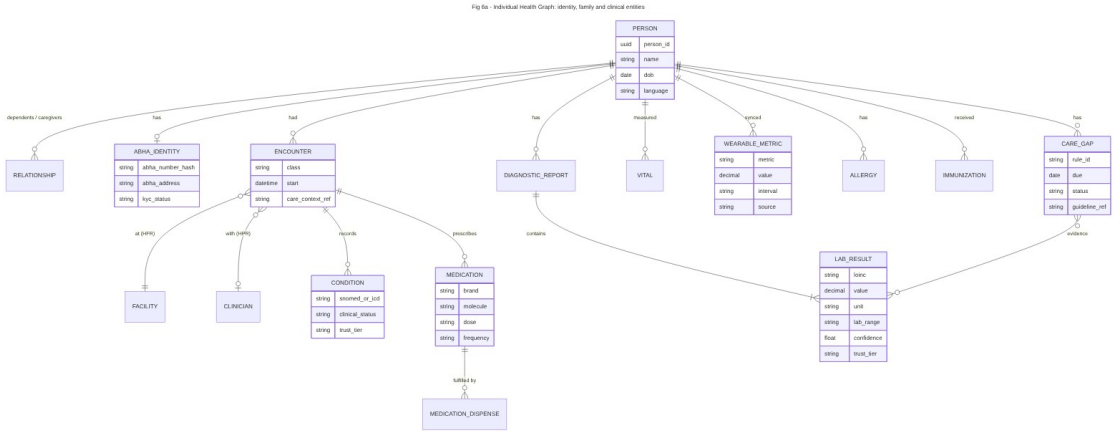


Fig 6b — Health Graph: insurance, money, consent and provenance

Insurance entities with clause references (coverage, exclusions, waiting periods), claims linked to encounters and expenses, the Coverage-to-Care link from care gaps to benefits, and consent records authorising source artefacts that provide provenance for every clinical node. Report refs: §6.3 F–G, §8.2.

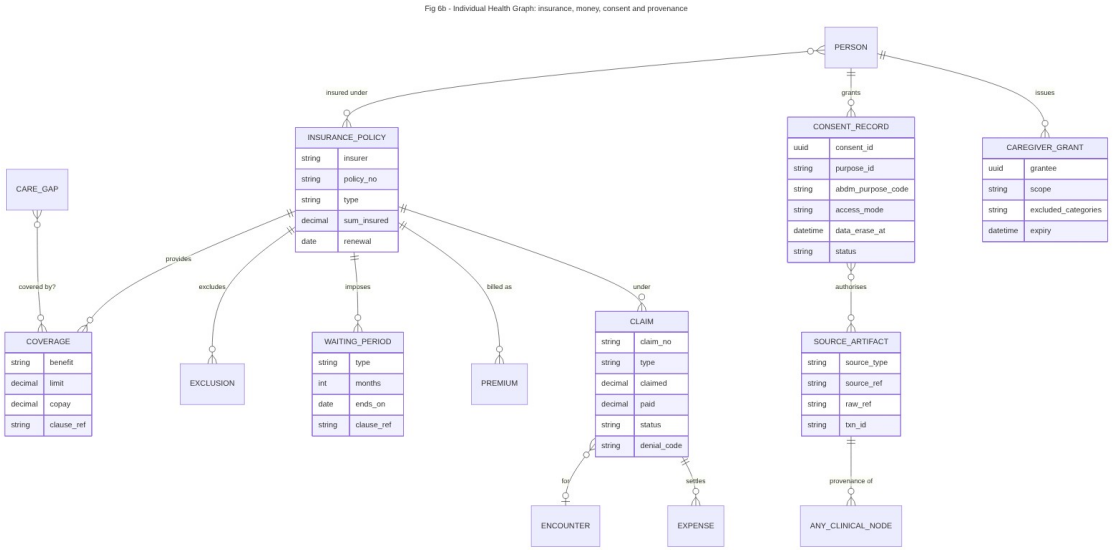


Fig 7 — Security zones and data classification

Zone separation by classification: C4 restricted (raw bundles, documents, identifiers, mental-health data) under per-person, per-source keys in KMS/HSM; C3 normalised clinical data; C1 de-identified analytics only from consented purposes. SIEM/SOC covers 6-hour CERT-In reporting and 180-day India log retention. Workforce has no standing C4 access. Report refs: §9.3, §9.5.

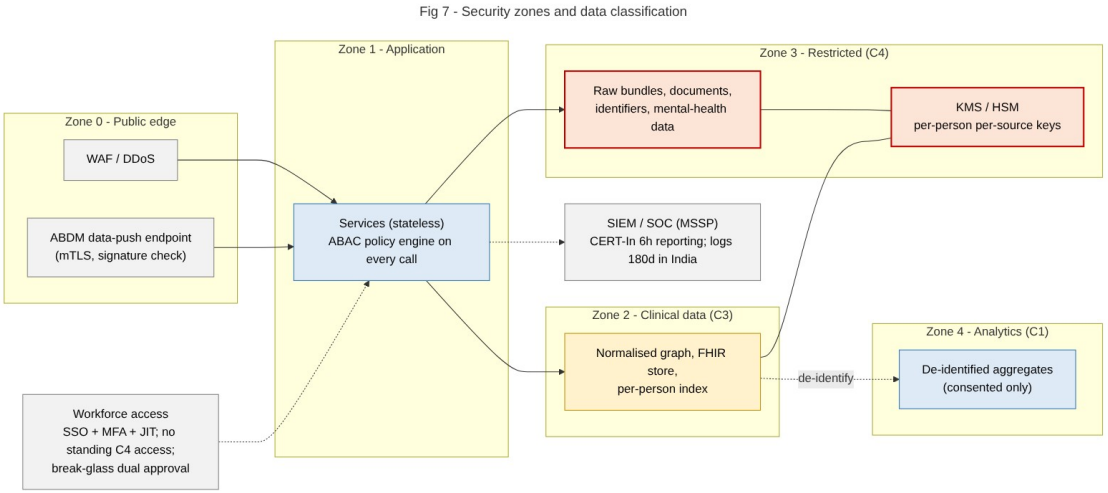
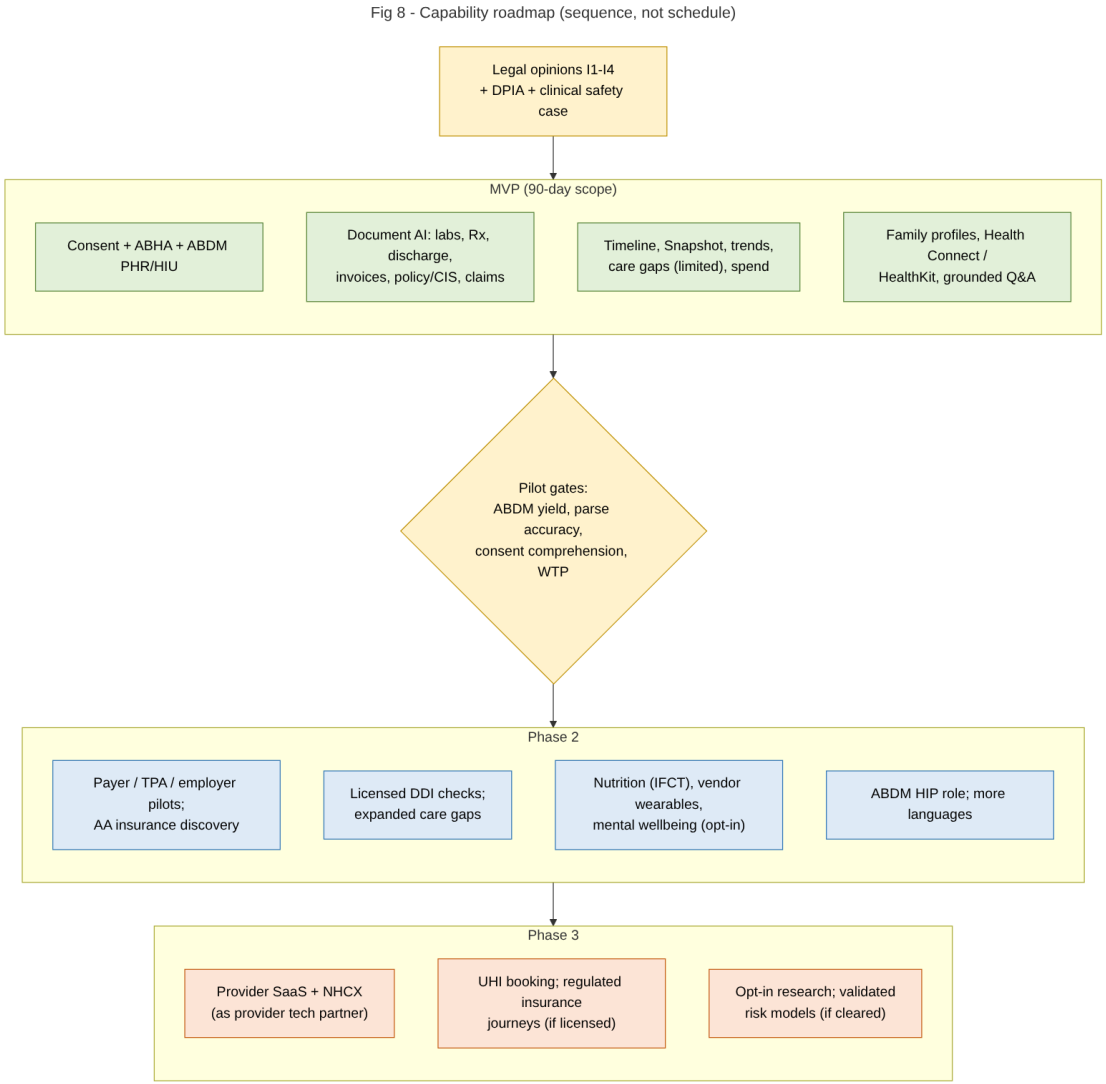


Fig 8 — Capability roadmap (sequence, not schedule)

Legal opinions, DPIA and the clinical safety case gate the MVP. Four pilot measures (ABDM yield, parse accuracy, consent comprehension, willingness to pay) gate Phase 2 investment. Phase 3 brings provider SaaS with NHCX participation as a provider technology partner, UHI booking, and regulated insurance journeys only if licensed. Report refs: §11.



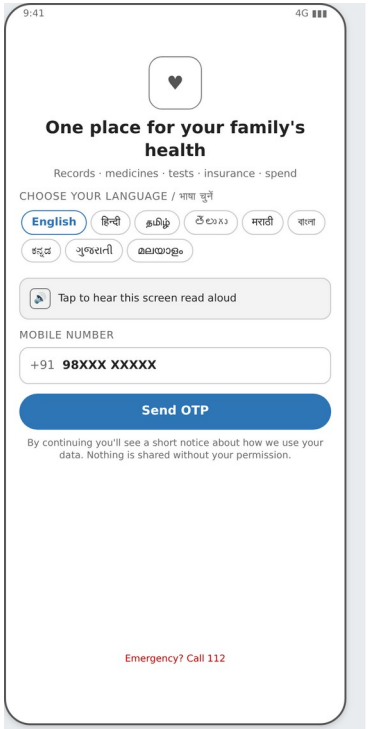
Part B — MVP wireframes (low fidelity)

Twelve Android-first screens covering the report's eight journeys (§7). Conventions:

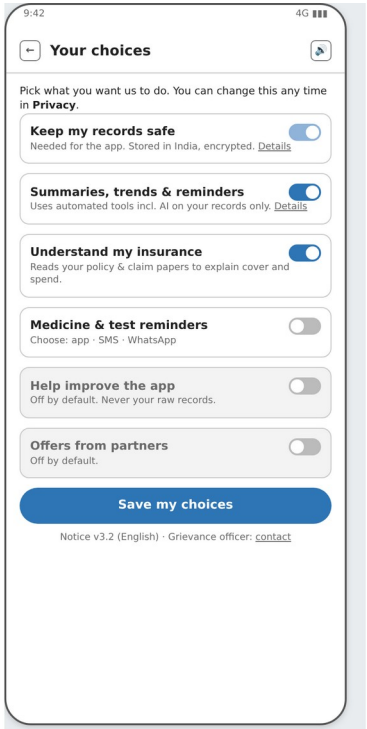
- Trust-tier badges on every data item: Verified clinical · From your document · Device · You entered · Insight.
- Family switcher on every screen.
- Non-diagnostic language throughout.
- An emergency route is always available.
- No insurance purchase, renewal or upgrade calls to action (pending the IRDAI opinion).

Screen	Journey	Key design rule
W01 Welcome & language	Onboarding	Vernacular first; read-aloud; ABHA not required to start
W02 Your choices	Onboarding / consent	One toggle per purpose; optional purposes off by default
W03 Find my records	ABHA linking	Narrow consent: chosen HIPs, explicit date range and erase date; honest partial delivery
W04 Home / Snapshot	Health Financial + Clinical Snapshot	Tier badges; doctor share is time-bound and view-only
W05 Timeline	Timeline	Episodes group visits, tests and claims; data-coverage statement
W06 Check values	Lab report / prescription upload	Source crops; drug lines always confirmed; "whose report is this?"
W07 Insurance	Policy upload	Clause-cited limits; computed waiting periods; interpretation disclaimer
W08 Claim	Claims upload	Document-driven status; deductions explained with clauses
W09 Ask	Q&A	Grounded, cited answers; rules compute numbers; feedback
W10 Family	Family view	Adults consent in their own right; scoped grants; minors via parental consent
W11 Privacy & consents	Withdrawal & deletion	Consequences shown first; export; crypto-shred + receipt
W12 Emergency	Safety	Red-flag interrupt before any AI generation; one-tap calls

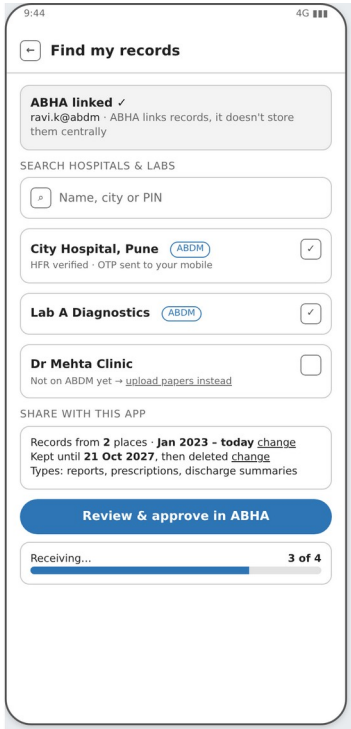
W01–W03: Welcome, consent choices, ABHA record discovery



W01 Welcome & language. Vernacular first; read-aloud for low literacy; OTP with SMS/IVR fallback. No ABHA required to start (§7.2 step 1–2).

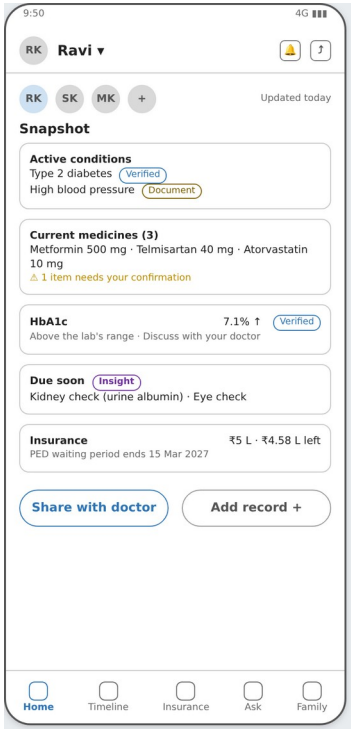


W02 Unbundled consent. One toggle per purpose (P1–P12, §5.4); no pre-ticked optional purposes; "Help improve" and "Offers" off. Receipt sent after save. Avoids CCPA dark patterns.

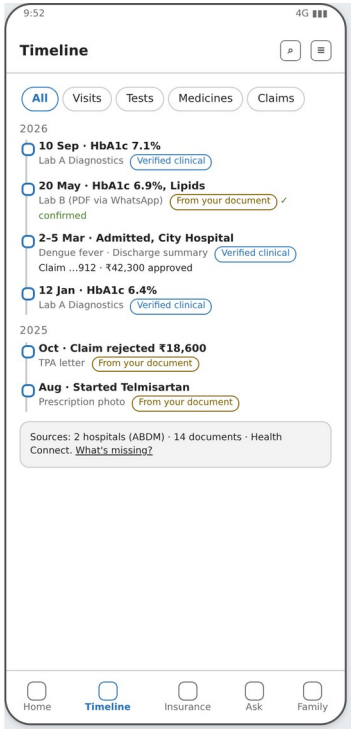


W03 ABDM discovery & self-access consent. Narrow by default: chosen HIPs, explicit date range and erase date (dataEraseAt). Honest partial-delivery status. Non-ABDM provider → upload path (§7.2 steps 3–5).

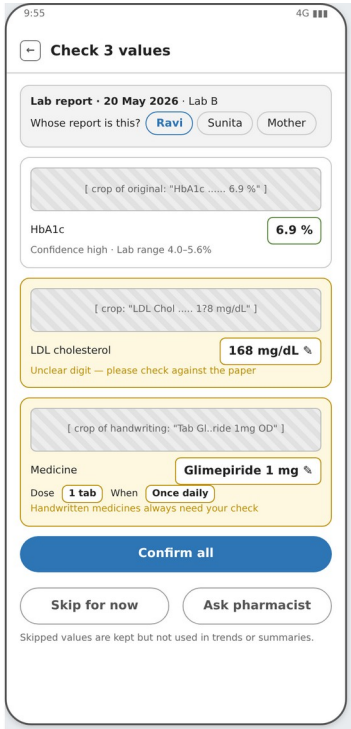
W04–W06: Snapshot, timeline, document confirmation



W04 Home / Health Financial + Clinical Snapshot. Family switcher on every screen; tier badges on every item; non-diagnostic language; quick doctor-share (time-bound, VIEW) (§7.6).

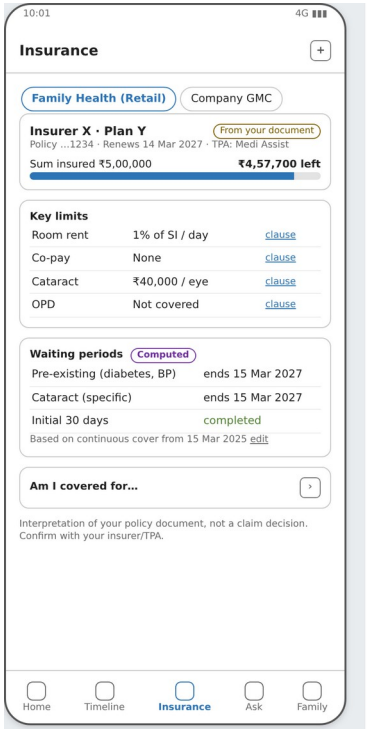


W05 Unified timeline. Episodes group admissions with tests and claims; every event shows its source; data-coverage statement prevents false completeness (§8.2).

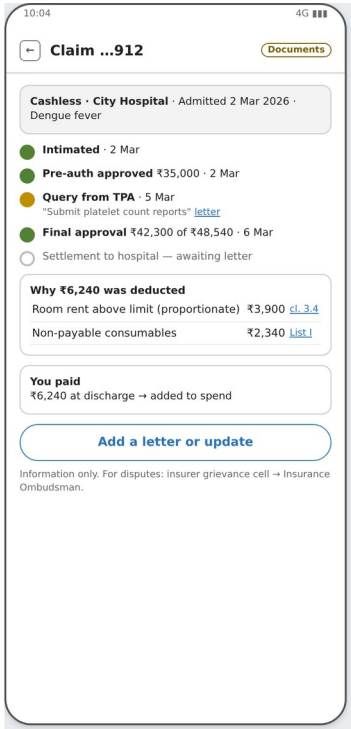


W06 Document confirmation (human-in-the-loop). Side-by-side source crops; drug lines always confirmed; person-assignment prompt for shared family phones; skipped data excluded from insights (§6.5, §10.4).

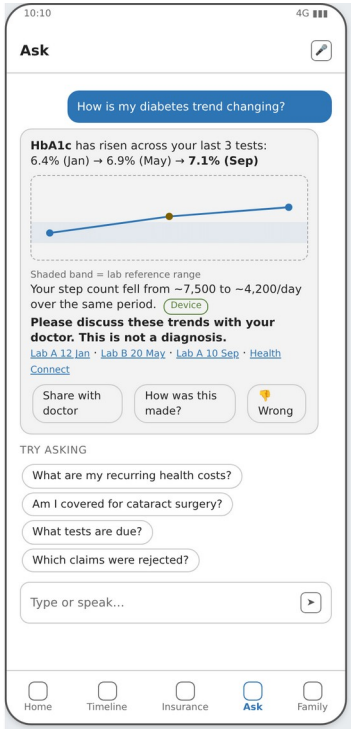
W07–W09: Coverage card, claim tracker, grounded Q&A



W07 Coverage card. Every limit links to the highlighted clause; waiting-period end dates computed from continuous-cover start; no buy/renew/upgrade CTA until IRDAI opinion (§7.4, §9.6).

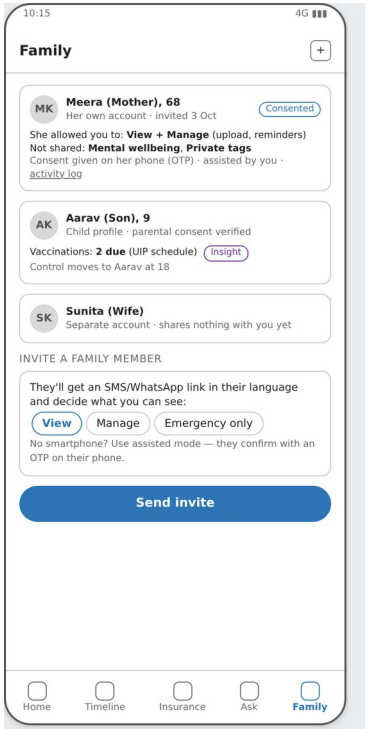


W08 Claim tracker. Document-driven status (NHCX not available to consumer apps); deductions explained line by line with clause references; feeds out-of-pocket spend (§7.4 step 6).

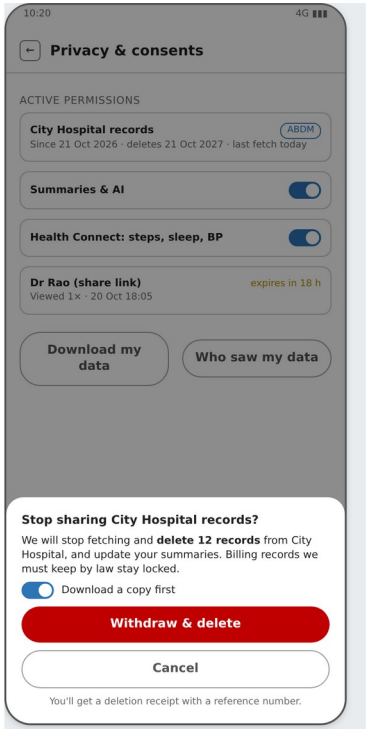


W09 Grounded Q&A. Answers only from the user's consented records; every claim cited; numbers from rules engine; tier badges; non-directive language; feedback loop (§7.7, §8.4).

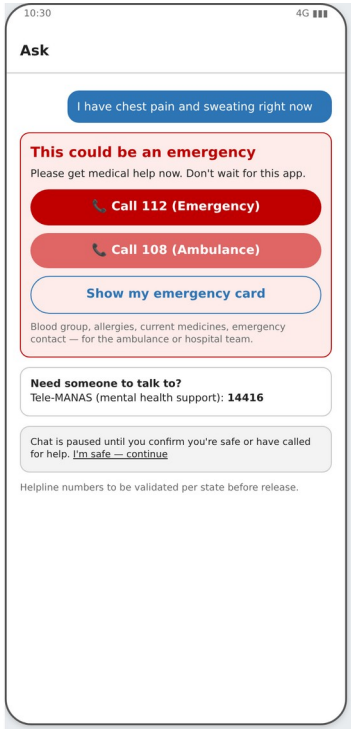
W10–W12: Family grants, consent withdrawal & erasure, emergency interrupt



W10 Family & caregiver grants. Adults consent in their own right with scoped grants; minors via verifiable parental consent; sensitive categories excluded by default; hand-over at 18 (§7.8).



W11 Consent dashboard, withdrawal & erasure. All ABDM and platform consents in one place; consequences shown before withdrawal; export first; crypto-shred + receipt (§7.9).



W12 Emergency interrupt. Red-flag detection precedes any AI generation; one-tap calls; emergency card uses the medical-emergency legitimate use; no triage advice (§9.4).