Caraway Care Platform

Multi-tenant home-care platform for carer visit logging, family wellbeing dashboards, and agency scheduling with compliance reporting.

~29-min read · 63 pages

INDUSTRY	PREPARED FOR	VERSION
Healthcare — domiciliary (home) care	Caraway Care (illustrative)	0.1

Status: for review · Sample — illustrative Scoping Sprint SDD (anonymized real engagement)

HOW WE START
Discovery
Fixed-price scoping — then build

MVP BUILD
~28 weeks
6 phases · delivered iteratively

FUNCTIONAL REQS
29
Core features in MVP scope

A SCOPING STARTING POINT — NOT A FIXED-PRICE QUOTE
Grounded in our delivery experience, this is a shared first read of the architecture, scope, and effort — a starting point to react to, not a fixed-price quote. The validated plan, wireframes, and a fixed-price Statement of Work come out of a paid Discovery phase. (See the closing section for how that works.)

Generated 2026-06-16 for Caraway Care (illustrative)

Sample — illustrative Scoping Sprint deliverable (anonymized engagement)

A NOTE FROM MINA

On scope, and what comes next.

This Scoping Sprint document was produced by a senior DBBS architect with our engineering team — built on the patterns from the products we have shipped over the years, our own production scope documents, and the standards a serious build is held to. It reflects how DBBS actually scopes and ships software.

What you are holding is our considered read of your build — specific, grounded, and honest about what we would still pressure-test with you. It is the foundation the team builds from on day one.

Building something brand-new can feel like betting on a long blueprint. The structure we are handing you is the bet we would take on a from-zero engagement: aggressive on shipping, conservative on assumptions.

If this lines up with what you are building, **book a slot on my Calendly** — or just reply and our team reads every message.

Mina Morkos
Business Development Manager, DBB Software

Contents

22 sections · click any entry to jump to that section, or use your PDF viewer's bookmark sidebar (left panel) to navigate.

TL;DR

- Building a multi-tenant SaaS platform for UK domiciliary care agencies, enabling mobile visit logging for carers, wellbeing dashboards for families, and compliance reporting for agency staff.
- Start with a ~16-week validation MVP focused on core visit logging and family transparency for one region, then scale to the full rollout over ~28 weeks.
- Automated medication administration records (eMAR) and visit invoicing/payroll are explicitly out of scope for the initial MVP.

PHASED DELIVERY — START LEAN, THEN SCALE

START LEAN

~16 weeks

Core carer mobile app for visit logging, rule-based wellbeing signal, and basic family dashboard/agency scheduling for a single region (CQC-compliant).

FULL ROLLOUT

~28 weeks

Full multi-tenant platform with comprehensive compliance reporting, scalability optimizations, and full NHS DSP Toolkit adherence for UK-wide rollout.

EXECUTIVE SUMMARY

Executive Summary

The Caraway Care Platform is designed as a Modular Monolith with LLM Agent Integration — a single deployable NestJS application composed of well-defined domain modules, with AI capabilities provided by an external LLM (e.g., Claude or GPT) invoked via API through an agentic workflow. This architecture maximises development speed (BD1) while maintaining the structural boundaries necessary for future module extraction and compliance auditing (BD2), and eliminates the need for a dedicated AI/ML engineer or custom model training. All technology decisions trace to the four business drivers:

Caraway Care aims to replace fragmented manual processes with a unified multi-tenant SaaS platform for UK domiciliary care. The platform will provide mobile tools for carers to log visits and observations, offer families transparent wellbeing dashboards, and automate scheduling and compliance reporting for agency staff. We recommend focusing the initial MVP on CQC compliance for England only, deferring RQIA expansion until the core platform is validated, to accelerate market entry and streamline regulatory overhead.

1. ABBREVIATIONS

Abbreviations

TERM	DEFINITION
ADR	Architectural Decision Record
CQC	Care Quality Commission (England)
DSPT	Data Security and Protection Toolkit (NHS)
eMAR	Electronic Medication Administration Records
GDPR	General Data Protection Regulation (UK)
GPS	Global Positioning System
LLM	Large Language Model
MVP	Minimum Viable Product
PHI	Protected Health Information
QA	Quality Assurance
RQIA	Regulation and Quality Improvement Authority (Northern Ireland)
SaaS	Software as a Service

2. PROJECT CONTEXT

Project Context

Background

The UK domiciliary care sector is under significant and growing pressure. The ageing population means that by 2030, one in five UK residents will be over 65. An estimated 88–97% of older adults express a preference to remain in their own homes rather than move into residential care, yet most care providers lack the digital tools to deliver safe, transparent, and efficient home-based care. The sector faces a workforce crisis with approximately 165,000 vacancies, compounding the documentation burden and compliance pressure on existing carers. Post-COVID behavioural shifts have further accelerated demand for remote monitoring and digital care solutions. The UK domiciliary care market was valued at approximately GBP 9.5 billion in 2023 with a compound annual growth rate of 4%. The broader UK homecare sector is projected to reach GBP 35 billion by 2030. The UK government is actively prioritising technology-enabled care through NHS Digital Social Care reforms, creating a favourable policy environment for digital care platforms. Northern Ireland (NI), the initial target market for Caraway, has a domiciliary care sector valued at GBP 300 million annually, serving over 25,000 clients. The Serviceable Available Market (SAM) for digital-enabled home-care technology is estimated at GBP 1.5 billion across the UK.

Goal

Deliver a secure, compliant, multi-tenant platform that streamlines care operations, enhances family transparency, and supports agency growth across the UK, starting with a pilot in one region.

Target Users

Carers, Family Members of Clients, Agency Staff (Managers, Administrators)

Business Drivers

Operational Efficiency	Automate manual processes like visit logging, scheduling, and compliance reporting to reduce administrative burden on agency staff and carers.
Enhanced Transparency	Provide families with real-time updates on care visits and a clear view of their relatives' wellbeing trends, building trust and peace of mind.
Regulatory Compliance	Ensure adherence to CQC (and future RQIA) regulations, NHS DSP Toolkit standards, and UK GDPR for data security and reporting.
Scalability	Build a multi-tenant platform capable of supporting expansion from a single pilot region to UK-wide operations without requiring a costly rebuild.

Market Context & Comparable Platforms

The UK domiciliary care market is undergoing digital transformation, driven by increasing regulatory scrutiny and the need for greater efficiency and transparency. Many agencies still rely on a mix of manual processes and generic tools, leading to operational inefficiencies and challenges in demonstrating compliance. There is a growing demand for integrated platforms that can streamline operations while providing better communication with families.

CarePlanner	Offers comprehensive care management, scheduling, and invoicing, but its family communication features are less emphasized than Caraway Care's proposed dashboard.
Care Control	Provides digital care planning, eMAR, and reporting, but may not offer the same depth of family-facing wellbeing insights or multi-tenant flexibility.
Birdie	Focuses on care management, a family app, and reporting, positioning itself similarly but without the explicit AI-driven decline detection roadmap.

How this build differs: Caraway occupies a unique position as the unified care + AI + community intelligence platform that bridges the gap between:

Open Questions — to address BEFORE Discovery

The answers to these questions firm up the scope before a paid Discovery phase kicks off. Treat them as homework — not nice-to-haves. Each one unblocks a specific scoping decision.

OQ-001
What specific CQC/RQIA reporting formats are required for compliance dashboards?
Impact: Compliance dashboard may not meet regulatory expectations

OQ-002
What is the expected pilot data volume? (recipients, visits/day, agencies)
Impact: Infrastructure sizing may be over/under-provisioned

OQ-003
Does the client have preferred branding guidelines?
Impact: Generic DBB design system applied; re-branding effort later

OQ-004
Clinical validation criteria for AI decline detection accuracy?
Impact: LLM agent outputs reviewed manually until validation criteria defined

OQ-005
Does the client have a self-trained LLM, or will the platform use an existing LLM provider (e.g., GPT, AWS Bedrock) via an agent for wellbeing data analysis? Given the task is structured numerical analysis, a general-purpose LLM with an agentic workflow is likely sufficient — confirm client preference.
Impact: Delays AI agent integration approach; rule-based scoring unaffected

OQ-010
Auth0 enterprise plan pricing and HIPAA BAA timeline
Impact: Auth provider selection blocked. Fallback: AWS Cognito

OQ-006
Which specific NHS APIs are required? Accreditation status?
Impact: NHS integration deferred; manual data entry in MVP

OQ-007
Monthly infrastructure budget for third-party services?
Impact: Services at default tiers; cost surprises possible

OQ-008
Scope deferral approval — 5 requirements deferred (see Section 6)
Impact: Acceptance criteria mismatch at delivery

OQ-009
Competitor research references from client?
Impact: Market positioning based on public info only

3. SCOPE & REQUIREMENTS

Scope & Requirements

In Scope (MVP)

- Carer mobile application for visit management (clock-in/out, activity logging, concern flagging)
- Family web dashboard for visit confirmation and wellbeing trends
- Agency web portal for carer scheduling, availability management, and compliance reporting
- Multi-tenant architecture supporting multiple care agencies
- Rule-based wellbeing signal generation from carer observations
- UK GDPR and NHS DSP Toolkit compliance, with CQC-specific reporting capabilities

Out of Scope (deferred)

- ~~Medication administration records (eMAR) are deferred to a later phase to focus the MVP on core visit management and family transparency.~~
- ~~Visit invoicing and payroll generation are deferred to a later phase, allowing the MVP to validate core operational workflows first.~~
- ~~Advanced AI-assisted decline detection using Large Language Models is a future roadmap item, building upon the initial rule-based system.~~
- ~~Integration with external HR, payroll, or accounting systems is deferred beyond the MVP to maintain a lean scope.~~

Success Metrics

CARER ADOPTION RATE

80% of active carers using the mobile app for visit logging within 4 weeks of pilot launch

Track unique carer logins and completed visit logs via platform analytics.

FAMILY ENGAGEMENT

60% of active family members logging into the dashboard at least once per week within 8 weeks of pilot launch

Monitor unique family member logins and dashboard view events.

COMPLIANCE REPORT GENERATION TIME

Automated CQC-ready reports generated in under 5 minutes

Measure report generation time from the agency portal.

REDUCTION IN MANUAL ADMIN TIME

25% reduction in time spent by agency staff on scheduling and visit verification

Baseline current manual process time and compare with post-launch operational metrics.

Functional Requirements

FR-001 Mobile-friendly portal for carers to view assigned clients

P0 L

Log visits, complete forms, record wellbeing notes, and upload photos

- Carer can view assigned client list with today's schedule
- Visit log form captures: arrival/departure time, tasks completed, wellbeing notes, photos
- Form submission works offline and syncs when connectivity is restored

FR-002 Family portal for viewing real-time visit logs

P0 L

Wellbeing summaries, and task completion

- Family member can view daily care log for their loved one
- Wellbeing summary displays daily index score and trend
- Data is updated within 60 seconds of carer submission

FR-003 Chat/messaging between family members and care coordinators

P1 L

- Family member can send messages to assigned care coordinator
- Messages are timestamped and stored per client record
- Notification sent to recipient on new message

FR-004 Family member alert configuration for wellbeing changes

P1 L

- Family member can set thresholds for wellbeing index alerts
- Alert delivered via push notification and/or email
- Alert history viewable in the portal

FR-005 Rota management and shift scheduling for carers

P0 L

- Admin can create, edit, and delete shifts for carers
- Shifts assigned to specific clients with time slots
- Carers see their daily/weekly schedule in the app

FR-006 GPS-based check-in/check-out for carer visits

P0 L

- Carer location captured at check-in and check-out
- Location validated against client address (configurable radius)
- Timestamp and GPS data stored for compliance audit

FR-007 Automated timesheet generation from visit logs

P0 L

- Timesheets auto-generated from check-in/out data
- Admin can review and approve timesheets
- Export to CSV/PDF for payroll processing

FR-008 Compliance dashboards and checklists

P0 L

- Dashboard shows compliance metrics: visit completion rate, documentation completeness, overdue tasks
- Configurable checklists per care type
- Alerts for compliance violations or missed visits

FR-009 Automated reminders for upcoming visits and overdue tasks

P1 M

- Carers receive reminders 15/30 minutes before scheduled visits
- Admins notified of overdue visits or incomplete documentation

FR-010 Rule-based wellbeing scoring system

P0 XL

- Daily wellbeing index calculated per care recipient from visit data
- Score based on configurable rules: mood, mobility, nutrition, medication compliance
- Score displayed on family portal and admin dashboard

FR-011 AI-powered early decline detection

P1 L

- LLM agent analyses structured care data to detect decline patterns
- Alerts generated when decline risk is identified by the agent
- Agent response quality metrics tracked and reportable

FR-012 Predictive analytics dashboard for trends

P1 L

- Trend visualisation for wellbeing scores over time per client
- Aggregate trend views for admin across all clients
- Exportable reports for regulatory submissions

FR-013 Calendar and RSVP system for social and wellness events

P0 L

- Community coordinator can create events with date, time, location, capacity
- Care recipients and families can RSVP to events
- Calendar view shows upcoming events

FR-014 Volunteer management and attendance tracking

P1 L

- Volunteers can be registered and assigned to events
- Attendance recorded at events via check-in
- Reports on volunteer hours and participation rates

FR-015 Feedback collection from event participants

P1 M

- Post-event feedback form sent to participants
- Feedback aggregated and viewable by coordinator

FR-016 Central management dashboard for care agency managers

P0 L

- Overview of all carers, clients, visits, and compliance metrics
- Filterable by date range, carer, client, status
- Real-time data refresh

FR-017 Analytics and reporting for compliance and operations

P0 XL

- Pre-built reports: visit completion, compliance scores, timesheet summaries, wellbeing trends
- Custom date range selection
- Export to PDF and CSV

FR-018 Data export capabilities (PDF/CSV)

P0 L

- All report views exportable to PDF and CSV
- Bulk data export for regulatory submissions
- Export audit logged

FR-019 Role-based access control (RBAC) for all user types

P0 L

- Roles: Carer, Family Member, Admin/Manager, Community Coordinator, Super Admin
- Each role has defined permissions for data access and operations
- Role assignment managed by Admin

FR-020 GDPR and HIPAA compliant data storage and privacy

P0 L

- All PHI/PII encrypted at rest (AES-256) and in transit (TLS 1.3)
- Consent management for data processing
- Right to access, rectification, erasure implemented

FR-021 Multi-factor authentication for admin and healthcare roles

P0 L

- MFA required for Admin/Manager and Carer roles
- Support for TOTP authenticator apps
- MFA bypass only via Super Admin recovery flow

FR-022 Push notifications for appointments and schedule changes

P0 M

- Carers receive push notifications for upcoming visits and schedule changes
- Family members receive notifications for completed visits

FR-023 Email reminders for compliance and wellbeing events

P0 M

- Automated email reminders for overdue compliance tasks
- Wellbeing alert emails sent to family members when thresholds breached

FR-024 SMS alerts for emergencies and critical wellbeing changes

P1 M

- SMS delivery for critical alerts (emergency, significant wellbeing decline)
- SMS opt-in/opt-out per user preference

FR-025 CRUD operations for clients

P0 M

Carers, visits, and programmes

- Full lifecycle management for all core entities
- Soft delete with audit trail for healthcare data retention

FR-026 Real-time data sync via secure APIs

P0 M

- API responses reflect latest data within 5 seconds of update
- WebSocket or SSE for real-time dashboard updates

FR-027 Multi-tenant architecture for agencies and councils

P0 XL

- Each tenant (agency/council) has isolated data
- Tenant context enforced at API, application, and database layers
- Super Admin can manage tenants

FR-028 Cross-device support: web

P0 M

Mobile, and tablet

- Responsive web app functions on desktop, tablet, and mobile browsers
- Native-like mobile experience via PWA or React Native app

FR-029 Role-based dashboards tailored to each user type

P0 L

- Carer dashboard: today's schedule, quick log entry
- Family dashboard: loved one's wellbeing, recent visits, alerts
- Admin dashboard: compliance overview, team management, analytics
- Coordinator dashboard: event calendar, volunteer management

Integrations

- Google Maps API (for GPS location services in carer app)
- SMS Gateway (for potential future alerts or notifications)
- Email Service (for account management and notifications)

4. NON-FUNCTIONAL REQUIREMENTS

Non-Functional Requirements

NFR-001 — API response time (p50)
Target: < 200ms. Measured via APM monitoring (Sentry, CloudWatch). Standard: Google RAIL model, Apdex standard.

NFR-002 — API response time (p95)
Target: < 500ms. Measured via APM monitoring. Standard: Google Web Vitals, industry standard for "good" UX.

NFR-003 — API response time (p99)
Target: < 1,000ms. Measured via APM monitoring. Standard: SRE best practices for tail latency.

NFR-004 — Page load (LCP)
Target: < 2.5s. Measured via Lighthouse, Real User Monitoring. Standard: Google Core Web Vitals "good" threshold.

NFR-005 — Interactivity (INP)
Target: < 200ms. Measured via Core Web Vitals. Standard: Google Core Web Vitals "good" threshold.

NFR-006 — Layout stability (CLS)
Target: < 0.1. Measured via Core Web Vitals. Standard: Google Core Web Vitals "good" threshold.

NFR-007 — Database query time (p95)
Target: < 100ms. Measured via Database monitoring. Standard: PostgreSQL optimization benchmarks.

NFR-008 — Real-time data sync latency
Target: < 5 seconds. Measured via Application metrics. Standard: SSE/WebSocket standard for dashboard updates.

NFR-009 — Visit form submission (offline)
Target: < 3 seconds local save. Measured via Device testing. Standard: PWA offline-first standard.

NFR-010 — Concurrent users (MVP)
Target: 500. Measured via Sufficient for NI pilot with 2–5 care agencies. Standard: MVP/Startup tier per SaaS benchmarks.

NFR-011 — Concurrent users (Growth)
Target: 5,000. Measured via UK-wide expansion target. Standard: Growth tier per Datadog SaaS benchmarks.

NFR-012 — API requests/sec (MVP)
Target: 100. Measured via Per-instance baseline for NestJS backend. Standard: Node.js ~1K rps capacity.

NFR-013 — Background jobs/min
Target: 500. Measured via Wellbeing score calculations, notification dispatch. Standard: BullMQ benchmark.

NFR-014 — Database connections (MVP)
Target: 50. Measured via Connection pool via PgBouncer. Standard: PgBouncer standard pool config.

NFR-015 — Multi-tenant support
Target: 50 tenants (MVP), 500 tenants (growth). Measured via Row-level security with tenant_id. Standard: Multi-tenant SaaS standard.

NFR-016 — Transport encryption
Target: TLS 1.2+ (prefer 1.3). Measured via GDPR, HIPAA, OWASP. Standard: NIST SP 800-52, PCI DSS 4.0.

NFR-017 — Encryption at rest
Target: AES-256 for all PHI/PII fields. Measured via GDPR, HIPAA. Standard: NIST SP 800-175B.

NFR-018 — Password hashing
Target: Argon2id or bcrypt (cost 12+). Measured via OWASP. Standard: OWASP Password Storage Cheat Sheet.

NFR-019 — Multi-factor authentication
Target: TOTP-based MFA for admin and carer roles. Measured via HIPAA Security Rule. Standard: NIST SP 800-63B.

NFR-020 — Session timeout (idle)
Target: 15 minutes for healthcare roles, 30 minutes for family. Measured via HIPAA, OWASP. Standard: OWASP Session Management, PCI DSS.

NFR-021 — Access token expiry
Target: 15 minutes. Measured via OAuth 2.0 best practices. Standard: RFC 6749, RFC 6819.

NFR-022 — Refresh token expiry
Target: 7 days. Measured via OAuth 2.0 Security BCP. Standard: RFC 6819.

NFR-023 — Vulnerability scanning
Target: Weekly (automated), quarterly (manual pentest). Measured via SOC 2, ISO 27001. Standard: SOC 2 Type II.

NFR-024 — Dependency audit
Target: Daily (automated via Dependabot/Snyk). Measured via OWASP. Standard: OWASP Dependency-Check.

NFR-025 — Audit logging
Target: All PHI access and state changes logged with user, timestamp, action, and affected record. Measured via HIPAA, GDPR. Standard: HIPAA Security Rule §164.312(b).

NFR-026 — RBAC enforcement
Target: Every API endpoint protected by role-based middleware. Measured via Application security. Standard: OWASP Access Control.

NFR-027 — System uptime
Target: 99.9% (three nines) — ~8.7 hours downtime/year. Measured via Standard SaaS SLA for healthcare B2B platform. Standard: AWS/Azure/GCP compute SLA.

NFR-028 — Recovery Time Objective (RTO)
Target: < 4 hours (standard), < 1 hour (critical systems). Measured via Multi-AZ failover for database. Standard: AWS disaster recovery tiers.

NFR-029 — Recovery Point Objective (RPO)
Target: < 1 hour (standard), < 5 minutes (care visit data). Measured via Continuous replication for care data. Standard: AWS backup/replication standards.

NFR-030 — Error rate (5xx)
Target: < 0.1% of requests. Measured via Application monitoring. Standard: Google SRE error budget model (99.9%).

NFR-031 — Mean Time to Recovery (MTTR)
Target: < 1 hour. Measured via Incident response procedures. Standard: DORA "Elite" performer threshold.

NFR-032 — Backup frequency
Target: Daily (full), hourly (incremental) for care data. Measured via Automated via AWS Backup. Standard: AWS Well-Architected, ISO 27001.

NFR-033 — Backup retention
Target: 90 days (hot), 365 days (cold/archive). Measured via Regulatory retention requirements. Standard: GDPR + HIPAA audit requirements.

NFR-034 — GDPR compliance (UK)
Target: UK GDPR / Data Protection Act 2018. Measured via Full compliance. Standard: ICO registration, DPIA, DPO appointment.

NFR-035 — HIPAA compliance
Target: HIPAA Security Rule, Privacy Rule. Measured via Full compliance. Standard: BAA with cloud providers, annual risk assessment.

NFR-036 — NHS DSPT alignment
Target: NHS Data Security and Protection Toolkit. Measured via Annual submission. Standard: Self-assessment against 10 data security standards.

NFR-037 — CQC/RQIA regulatory readiness
Target: CQC Fundamental Standards / RQIA Standards. Measured via Platform supports compliance documentation and reporting. Standard: Compliance report generation, audit trail.

NFR-038 — WCAG 2.1 AA accessibility
Target: Web Content Accessibility Guidelines. Measured via All user-facing features. Standard: Lighthouse accessibility audit, manual testing.

Quality Attributes

The quality attributes that matter most for this product, ranked by priority and tied to a measurable criterion where one applies.

RANK	ATTRIBUTE	TARGET	WHY
P1	**Security & Compliance**	GDPR + HIPAA encryption, audit logging, MFA, RBAC	BD2 (Critical) — Healthcare data requires the highest security posture. Non-negotiable.
P2	**Reliability**	99.9% uptime, automated failover, data backup	BD2 — Care data must be available when needed; data loss is unacceptable in healthcare
P3	**Usability**	WCAG 2.1 AA, < 2-minute task completion for carers, progressive disclosure	BD4 — Platform adoption depends on ease of use for non-technical carers and elderly family members
P4	**Maintainability**	Modular architecture, 70%+ test coverage, structured logging	BD1 + BD3 — Fast development requires clean, testable code; scalability requires modular decomposition
P5	**Testability**	Automated unit/integration/E2E tests, CI/CD pipeline with quality gates	BD1 — Rapid iteration requires confidence in automated testing to maintain quality at speed

Monitoring & Analytics

OpenTelemetry-first instrumentation, shipped to Sentry (errors) + Vercel Analytics / CloudWatch (infra) + Langfuse (for future LLM traces).

- API latency and error rates (per endpoint)
- Carer app clock-in/out success rate
- Family dashboard load times
- Database query performance
- Wellbeing signal processing duration
- User login success/failure rates
- System uptime

Product analytics: Product analytics will track user engagement with key features (e.g., number of visits logged, family dashboard logins, report generations) to inform product iteration and identify areas for improvement.

Data Handling & Privacy

The personal-data classes this product handles, with the lawful basis, retention, and residency for each — the table a data-protection officer checks first.

DATA CLASS	LAWFUL BASIS	RETENTION	RESIDENCY
Client Personal Identifiable Information (PII)	Legitimate Interest (for care provision) and Explicit Consent (for sharing with family)	7 years post-service termination (NHS record keeping guidelines)	United Kingdom
Client Special Category Data (Health/Wellbeing Observations)	Explicit Consent and Substantial Public Interest (provision of health/social care)	7 years post-service termination (NHS record keeping guidelines)	United Kingdom
Carer PII (Contact, Employment Details)	Contractual Necessity (employment contract)	6 years post-employment termination	United Kingdom
Visit Logs (GPS, Timestamps)	Legitimate Interest (service verification, compliance)	7 years post-service termination	United Kingdom

5. CONSTRAINTS & ASSUMPTIONS

Constraints & Assumptions

Constraints

- UK data residency is a non-negotiable requirement for all data storage and processing.
- Compliance with UK GDPR and NHS DSP Toolkit is mandatory from the outset.
- The initial pilot must be live within approximately 7-9 months to align with the next care-commissioning cycle.
- The data model must be extensible to support future features like eMAR and invoicing without requiring a full rebuild.

Assumptions

- The initial pilot will focus solely on CQC compliance for England, deferring specific RQIA requirements to a later phase.
- Caraway Care will provide clear clinical rules and thresholds for the initial rule-based wellbeing signal generation.
- Carers will have access to a smartphone with internet connectivity during their shifts to use the mobile application.
- Agency staff will be responsible for initial data entry of client and carer profiles into the platform.
- The platform will be deployed as a single-tenant instance for the pilot, with multi-tenant capabilities enabled for broader rollout.

Dependencies

The external services and client inputs this build depends on — what a delivery lead confirms before committing to a date.

- Selected licensed sports/care data provider — contract signed and API credentials issued
- Auth0 Organizations tenant with a HIPAA BAA + UK-GDPR data-processing agreement in place
- Client-provided clinical rules and thresholds for the wellbeing scoring engine
- Apple App Store + Google Play developer accounts for the mobile app
- Pilot agencies and a carer cohort confirmed for UAT
- AWS account + eu-west-1 data-residency sign-off; NHS API accreditation (deferred to Phase 2)

6. PROPOSED TECHNICAL SOLUTION

Proposed Technical Solution

Architecture Overview

This diagram presents a C4-style container view of the Caraway Care Platform. It shows the three client applications (Next.js Web App, React Native Mobile App, and an Admin Dashboard) communicating over HTTPS with the NestJS API, which contains six internal domain modules: Care, Scheduling, Community, Admin, Auth and Tenant, and Notifications. The NestJS API connects to the Python FastAPI AI/ML Service for wellbeing scoring, PostgreSQL (RDS Multi-AZ) as the primary data store, Redis (ElastiCache) for caching and job queues, and five external services: Auth0, S3, CloudFront CDN, Twilio, Amazon SES, and Firebase Cloud Messaging. The platform uses a Modular Monolith pattern for the core application with a separate AI microservice, chosen to balance development speed (BD1) against the structural rigour needed for healthcare compliance (BD2). This diagram traces how data moves through the Caraway Care Platform, starting from carer and family user input on client devices, through the NestJS API and its domain modules, into PostgreSQL for persistence, and to the Python FastAPI AI/ML Service for wellbeing score computation. It shows the asynchronous event flow via Bull queues on Redis: when a care visit is completed, the event triggers the AI service to compute a wellbeing score, which is stored back in PostgreSQL and cached in Redis, and notifications are dispatched to family members via push, SMS, or email. Admin users view aggregated data through compliance dashboards that read from the database and cache layer. This diagram shows all system components grouped by layer: client applications (Next.js Web App, React Native Mobile App), the NestJS modular monolith with its six domain modules and cross-cutting Audit Layer, the Python FastAPI AI/ML microservice, data stores (PostgreSQL, Redis, S3), and all external integrations. Connection types are labelled: HTTPS REST for synchronous API calls, OIDC/OAuth 2.0 for authentication flows, Bull/Redis for async event queues, and specific SDK protocols for Twilio (REST), Amazon SES (AWS SDK), and Firebase Cloud Messaging (Admin SDK). Queue Infrastructure: Bull (backed by Redis ElastiCache) for all job queues. Bull provides delayed jobs, retries with exponential backoff, dead letter queues, and job prioritisation. Failed jobs retry 3 times with exponential backoff (1s, 4s, 16s), then move to dead letter queue. Queue monitori

Recommended Stack

FRONTEND	Next.js 16 (App Router) with React 19 and Tailwind v4 for web applications; React Native (Expo) for the mobile application.
BACKEND	Node.js (TypeScript) with NestJS on serverless (AWS Lambda) for API services.
DATABASE	PostgreSQL on AWS RDS (multi-AZ) for primary data storage; Redis for caching and queueing.
INFRA	AWS (eu-west-1 Ireland region) for hosting, Vercel for Next.js deployments.
OBSERVABILITY	OpenTelemetry-first instrumentation, shipped to Sentry (errors) and CloudWatch (infra).
THIRD-PARTY	Auth0 (for user authentication and authorization), Google Maps API (for GPS services), Email Service (e.g., AWS SES), SMS Gateway (e.g., Twilio)

Technology Evaluation

DECISION	SELECTED	ALTERNATIVES	WHY
Frontend Framework	**Next.js 16 (selected)**	Remix, Angular, Vue + Nuxt	Aligns with BD1 (DBB templates), BD4 (RSC for performance, shadcn/ui for accessibility)
Backend Framework	**NestJS (selected)**	Express.js, Spring Boot, Django	BD1 (DBB boilerplate), BD2 (structural module boundaries for compliance auditing)
Database	**PostgreSQL 17 on RDS (selected)**	Aurora PostgreSQL, MongoDB Atlas, CockroachDB	BD1 (cost-effective for pilot), BD2 (schema isolation + RLS), BD3 (read replicas for analytics)
Authentication Provider	**Auth0 (selected)**	AWS Cognito, Keycloak, Firebase Auth	BD2 (HIPAA BAA + Organizations for multi-tenant), BD1 (pre-built SDKs reduce auth code)

Architecture Decision Records

ADR-001. Cloud Platform — AWS

ACCEPTED

The Caraway Care Platform requires a cloud provider supporting HIPAA-eligible services, a UK/Ireland data centre for GDPR data residency, and managed services to accelerate time-to-pilot (BD1). The client has no existing cloud infrastructure.

Decision: AWS, deploying to eu-west-1 (Ireland).

ALTERNATIVES CONSIDERED

VIABLE	**Google Cloud Platform.** Strong AI/ML services; competitive pricing. Fewer HIPAA-eligible services; less DBB familiarity
VIABLE	**Microsoft Azure.** Strong NHS/healthcare UK presence; Azure AD. Less DBB experience; higher equivalent costs

ADR-002. Backend Framework — NestJS

ACCEPTED

The backend must support a modular monolith with clear domain boundaries, built-in cross-cutting concerns (auth, audit logging), and OpenAPI documentation. Must share TypeScript with the frontend.

Decision: NestJS with TypeScript.

ALTERNATIVES CONSIDERED

WEAK	**Express.js.** Lightweight; flexible. No enforced structure; manual OpenAPI; no DI system
VIABLE	**Spring Boot (Java).** Enterprise-grade; strong healthcare ecosystem. Different language from frontend; longer development cycles
WEAK	**Django (Python).** Good ORM; built-in admin. Different language from frontend; weaker TypeScript interop

ADR-003. Frontend Framework — Next.js 16

ACCEPTED

The web application serves multiple user roles with different UX needs. Some pages require SSR for performance (family dashboard), while others are static (community event listings). Accessibility (WCAG 2.1 AA) required for elderly users (BD4).

Decision: Next.js 16 with React 19, TypeScript, Tailwind CSS, and shadcn/ui.

ALTERNATIVES CONSIDERED

VIABLE	**Remix.** Full-stack React; good progressive enhancement. Smaller ecosystem; less DBB experience
WEAK	**Angular.** Enterprise features; strong typing. Larger bundles; steeper learning curve; not DBB preferred
WEAK	**Vue + Nuxt.** Good DX; lighter weight. Not DBB preferred; smaller enterprise ecosystem

ADR-004. Authentication Provider — Auth0

ACCEPTED

Requires OAuth 2.0/OIDC with MFA, RBAC, multi-tenant support. HIPAA compliance requires BAA with identity provider. Five user roles with different permission sets. Must support both web and mobile clients.

Decision: Auth0 with HIPAA BAA.

ALTERNATIVES CONSIDERED

VIABLE	**AWS Cognito.** AWS-native; lower cost. Poorer DX; limited RBAC; no Organizations equivalent
WEAK	**Keycloak (self-hosted).** Full control; no per-user cost. Operational overhead; self-managed HA; no managed BAA
WEAK	**Firebase Auth.** Easy mobile integration. No HIPAA BAA; limited RBAC

ADR-005. Database — PostgreSQL 17 on AWS RDS

ACCEPTED

Stores care records (PHI), user profiles (PII), scheduling data, community events, and audit logs. Multi-tenant data isolation is a hard requirement. Must support complex relational queries and ACID transactions. HIPAA requires encryption at rest and auditable access controls.

Decision: PostgreSQL 17 on AWS RDS Multi-AZ with schema-per-tenant isolation.

ALTERNATIVES CONSIDERED

VIABLE	**Aurora PostgreSQL.** Higher availability; faster replication. Higher cost; premature for pilot scale
WEAK	**MongoDB Atlas.** Flexible schema; good for rapid prototyping. Weaker ACID; harder compliance auditing; not relational
WEAK	**CockroachDB.** Distributed SQL; multi-region. Overkill for pilot; higher operational complexity

ADR-006. Mobile Framework — React Native with Expo

ACCEPTED

Mobile app used by carers (visit logging, GPS check-in, schedules) and family members (wellbeing dashboard, notifications). Offline support critical for poor-connectivity areas. Push notifications and background GPS required. Must run on iOS and Android.

Decision: React Native with Expo managed workflow.

ALTERNATIVES CONSIDERED

VIABLE	**Flutter.** Good performance; single codebase. Different language (Dart); no skill sharing with web team; conflicts BD1
WEAK	**Native (Swift + Kotlin).** Best performance; native APIs. Two codebases; doubled cost and timeline; conflicts BD1
WEAK	**PWA.** Single codebase; no app store. Limited offline; poor GPS background tracking; insufficient for check-in/out

ADR-007. AI Approach — LLM Agent via API (No Custom Model Training) ACCEPTED

Platform requires AI-driven wellbeing insights: (1) rule-based scoring aggregating care visit data into a deterministic wellbeing index, (2) decline detection identifying negative trends in care recipient wellbeing. The team does not include a dedicated AI/ML engineer, and custom model training is not desired. An existing LLM with agentic capabilities can analyse structured care data for pattern recognition.

Decision: Use an existing LLM (e.g., Claude or GPT) via API, invoked from the NestJS backend through an agent workflow. Rule-based scoring remains deterministic (no LLM). LLM agent is used only for decline detection and care insights.

ALTERNATIVES CONSIDERED

VIABLE **Python FastAPI + Scikit-learn.** Standard ML stack; full VPC isolation; no external API dependency. Requires AI/ML engineer; model training needs 3-6 months of data; second language in codebase; separate CI/CD

WEAK **AWS SageMaker.** Managed ML platform; auto-scaling endpoints. Requires ML expertise; significantly higher cost; overkill for current needs

WEAK **Self-hosted LLM (e.g., Llama).** Full data control; no external API costs. GPU infrastructure cost; operational complexity; model quality gap vs frontier models

Figure 1 — Data model

Entity Relationship Diagram

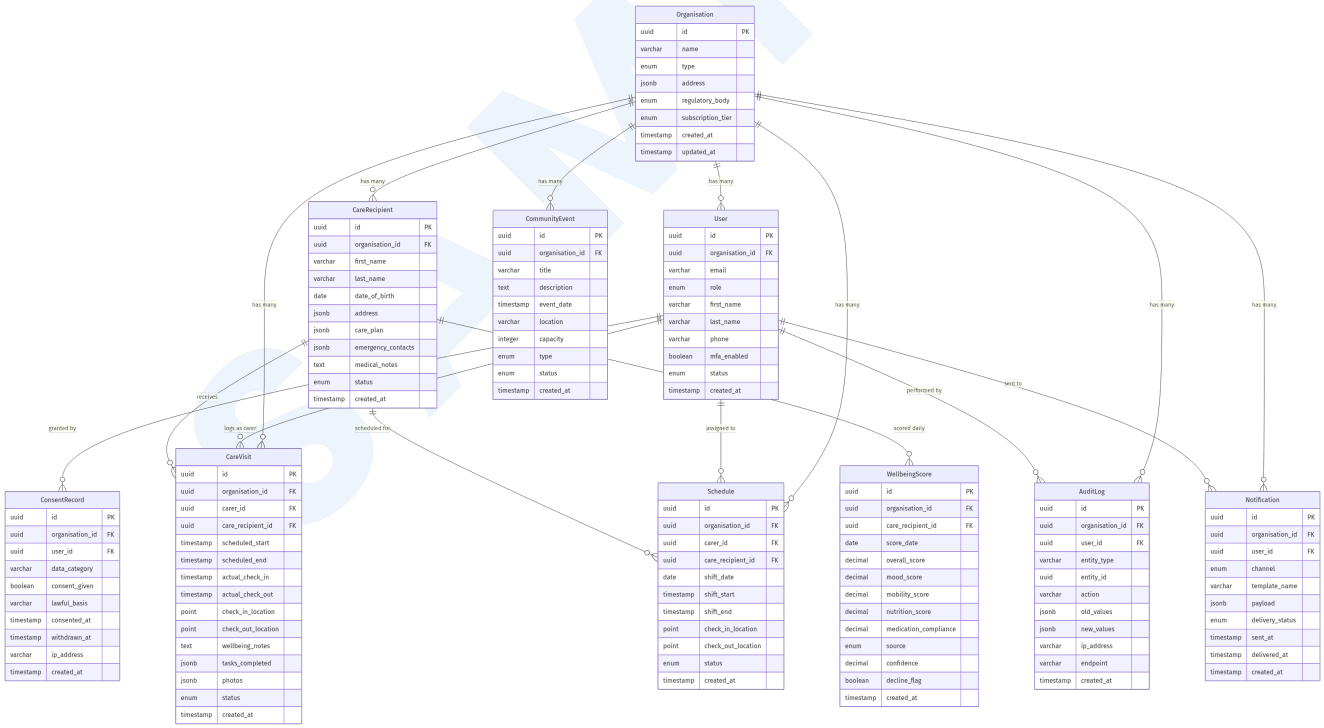


Figure 2 — Architecture

High-Level System Architecture

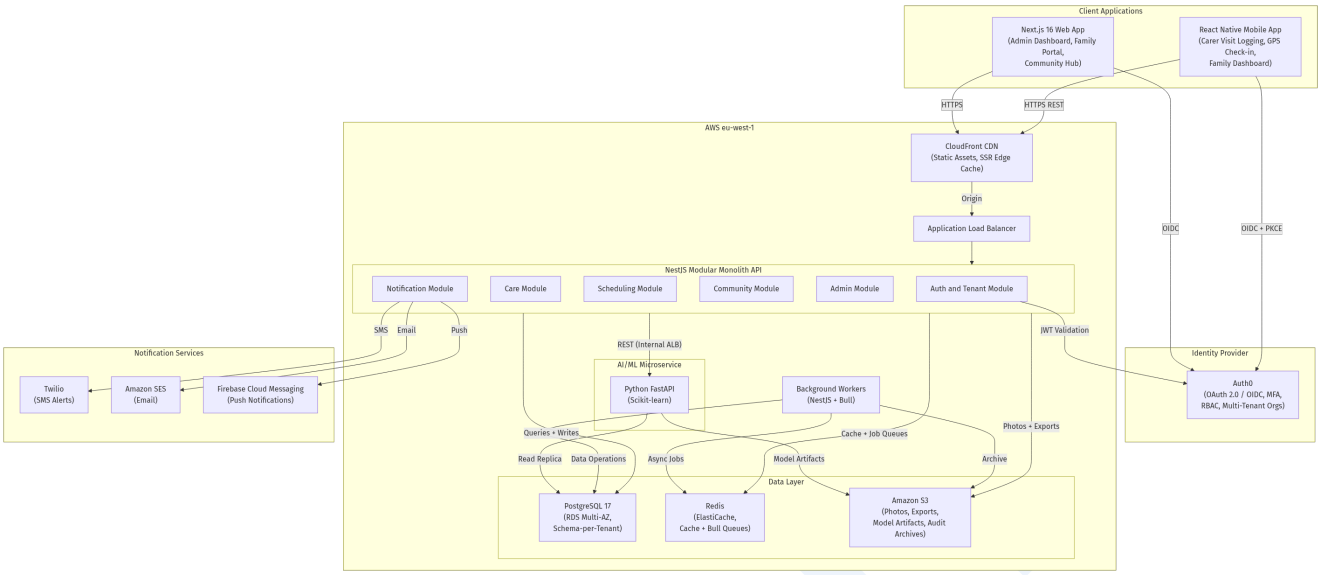


Figure 3 — Architecture

Data Flow Diagram

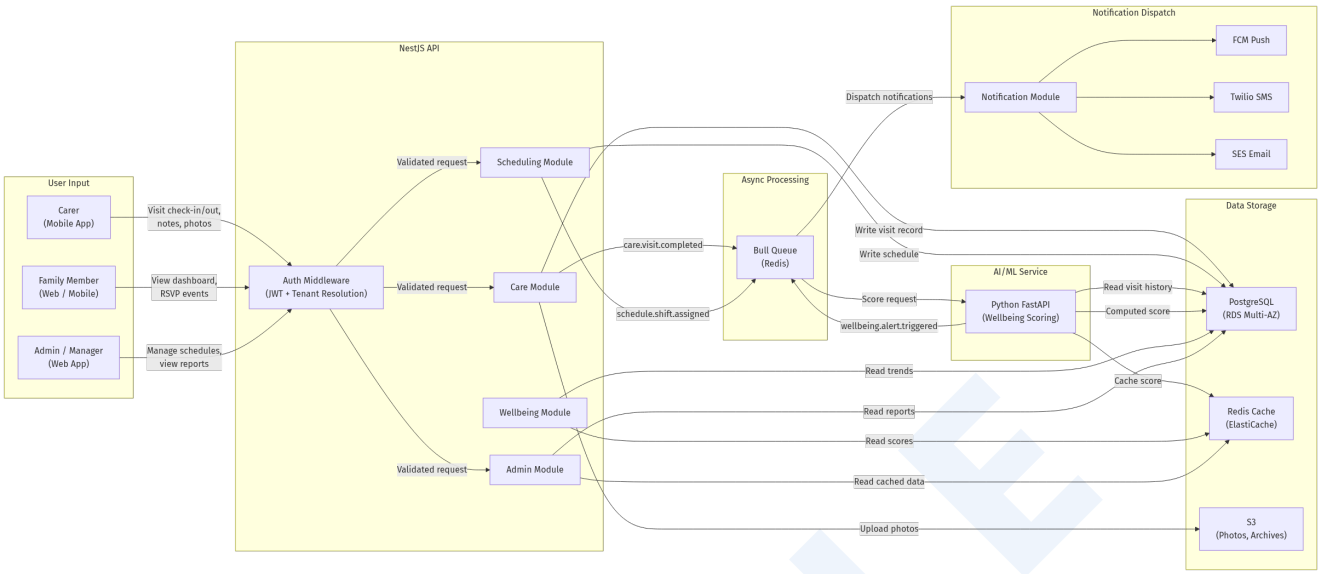


Figure 4 — Architecture

Component and Integration Map

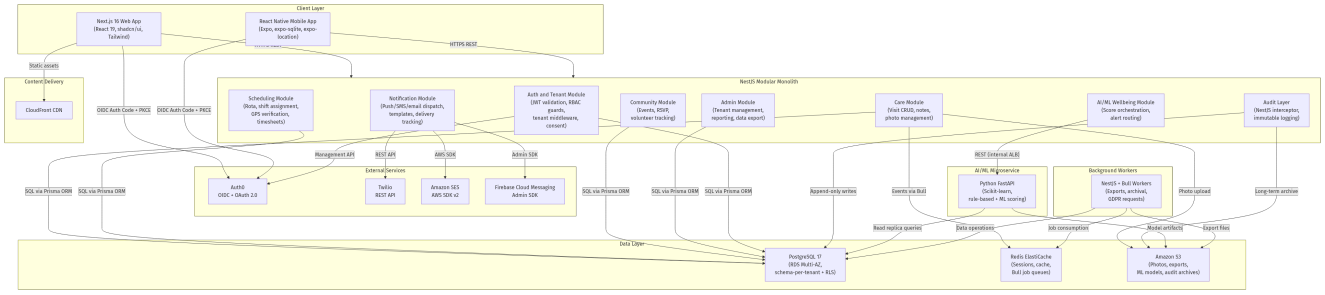


Figure 5 — Sequence

a. Care Visit Workflow

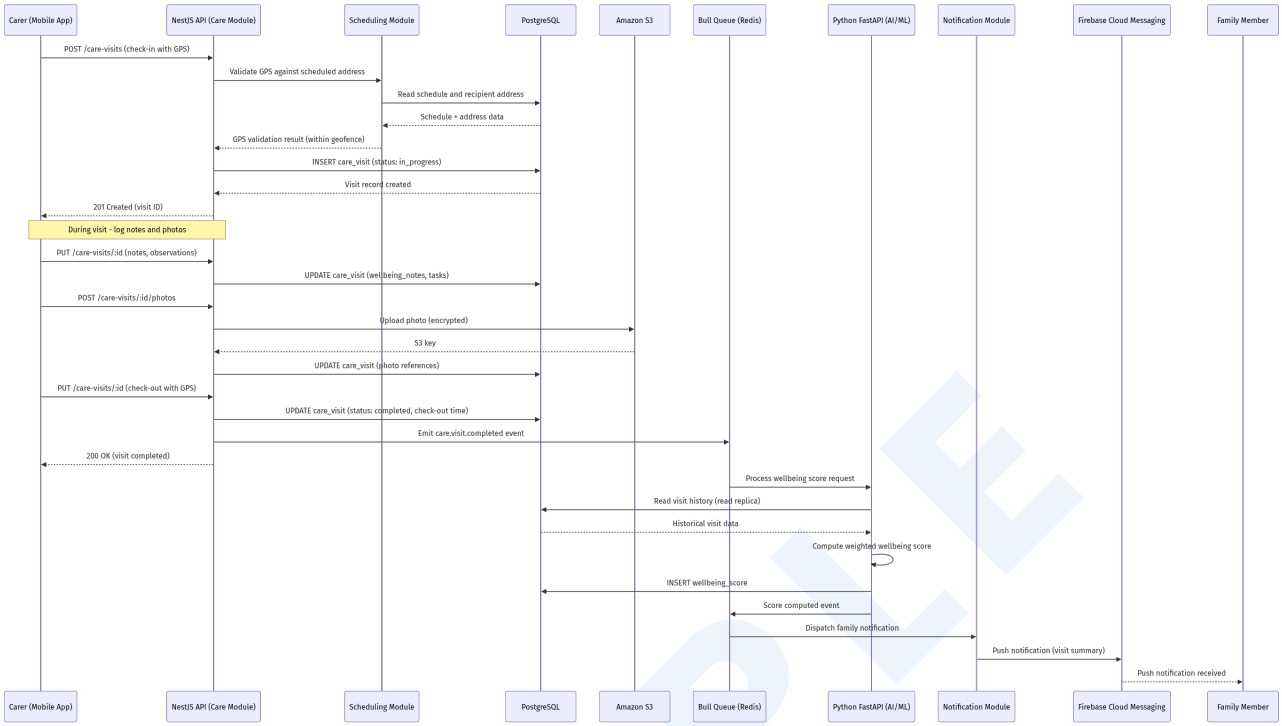


Figure 6 — Sequence

b. Wellbeing Alert Workflow

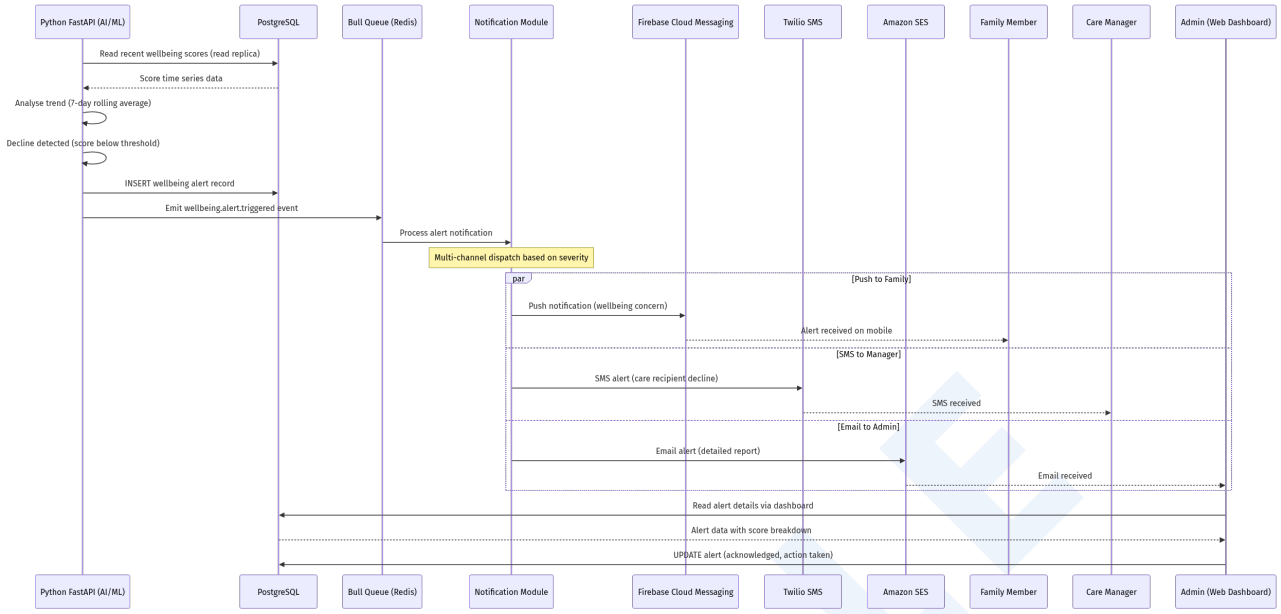


Figure 7 — Sequence

c. Scheduling and Compliance Workflow

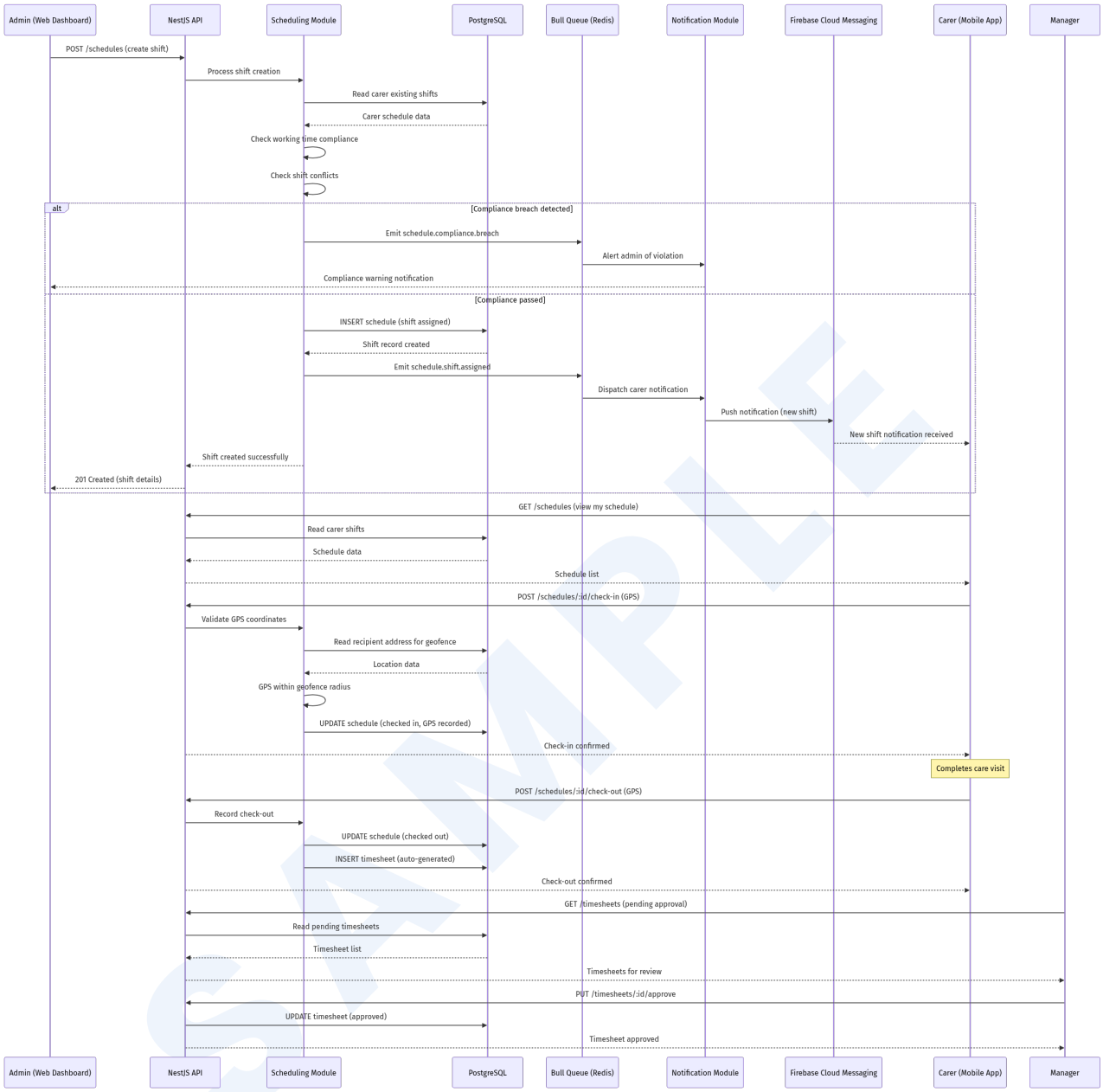


Figure 8 — Sequence

d. Authentication and Multi-Tenant Flow

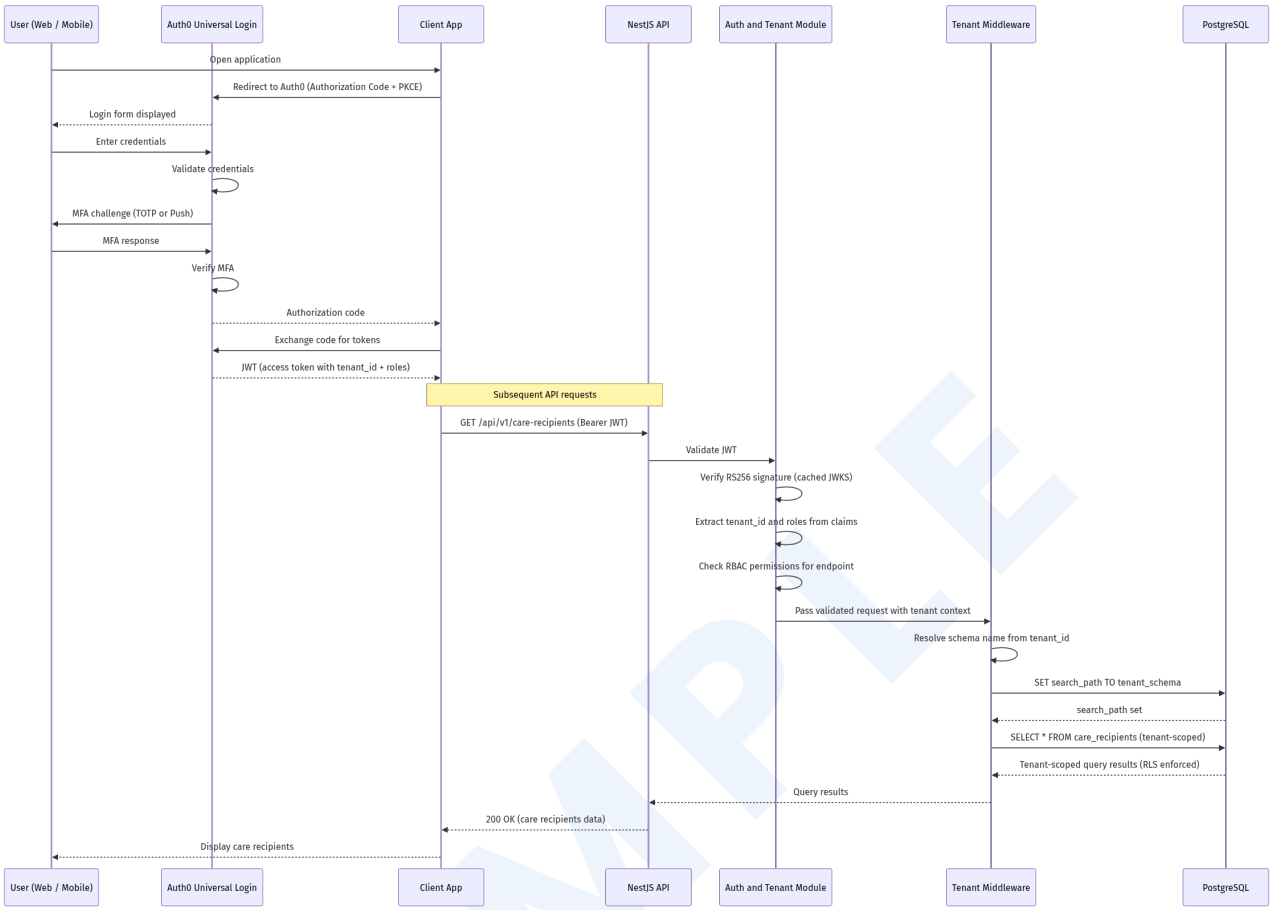


Figure 9 — Architecture

Deployment Architecture

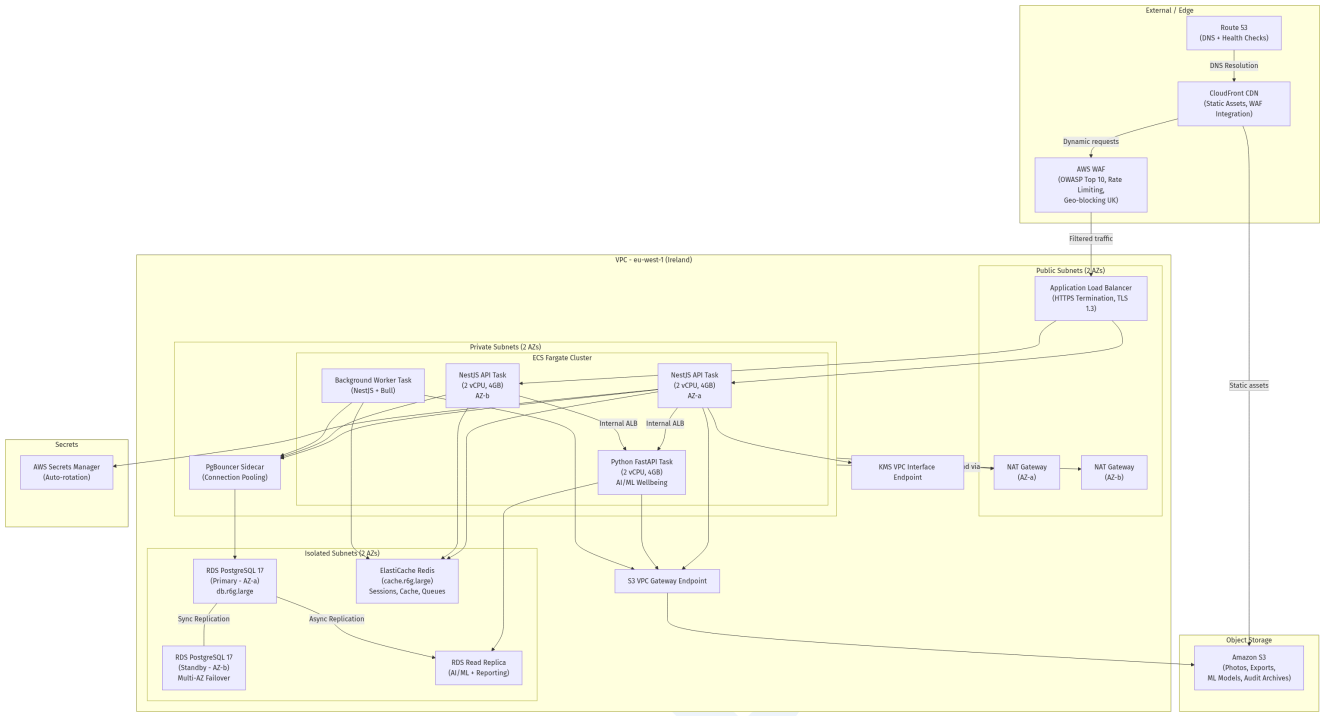


Figure 10 — Deployment

Deployment Topology

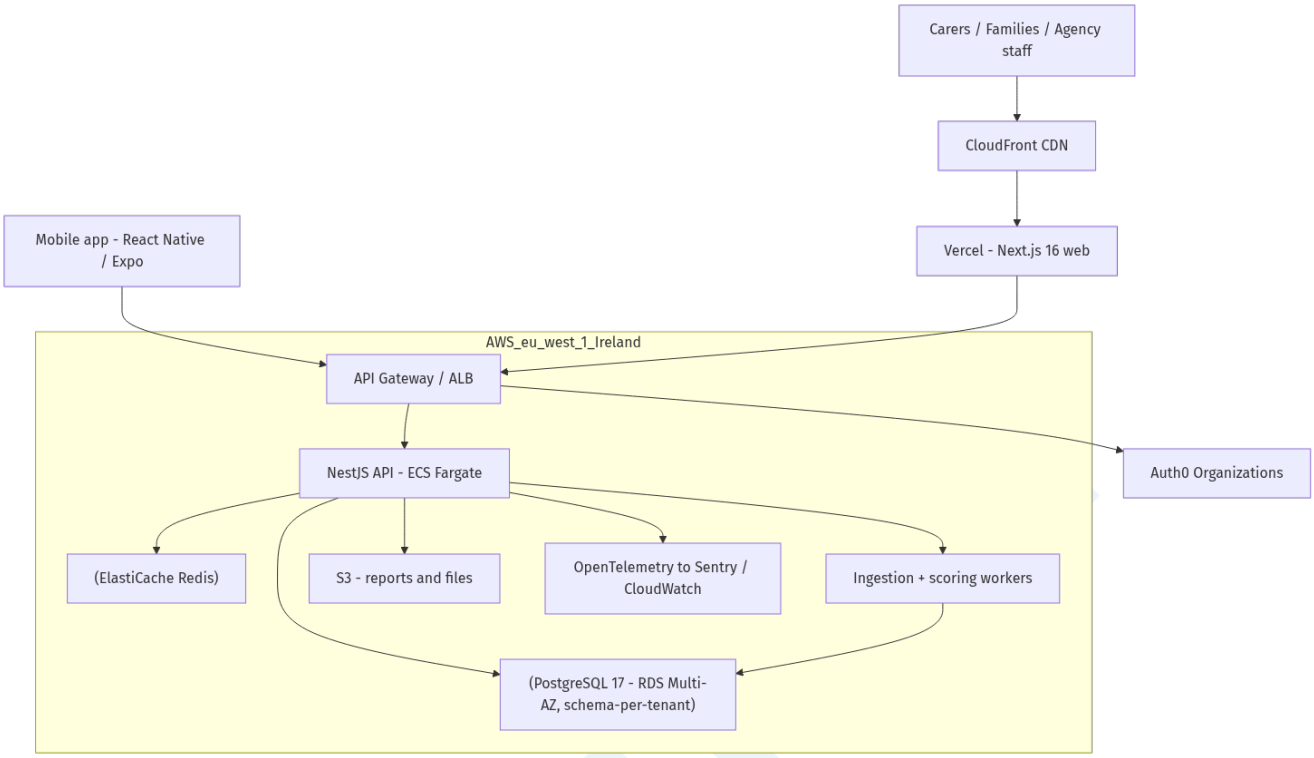


Figure 11 — Architecture

CI/CD Pipeline

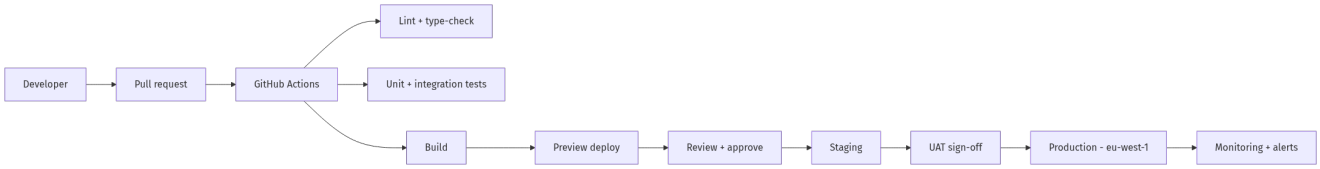
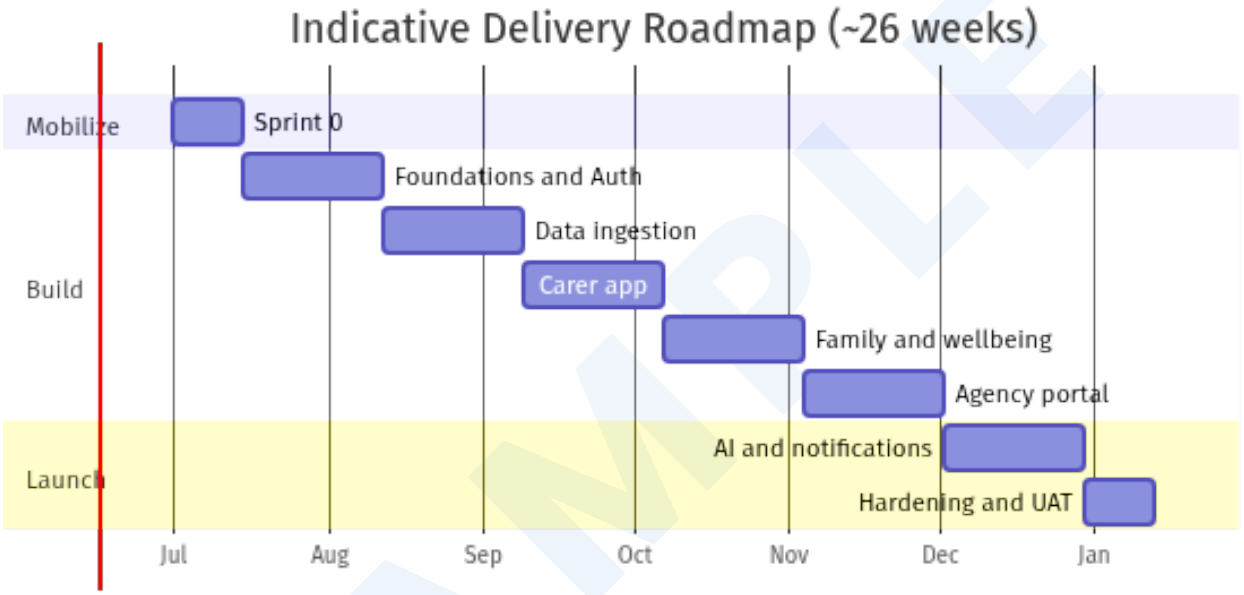


Figure 12 — Roadmap gantt

Indicative Delivery Roadmap



Worked Example

One concrete end-to-end trace of the primary workflow — how a real request flows through the system.

A carer completes a visit for a client, logs their activities and observations via the mobile app, and the family member then views the updated visit confirmation and wellbeing trend on their dashboard.

1. 1. Carer Clocks In

```
Carer 'Sarah Jones' arrives at client 'Evelyn Smith's' home at 09:00 on 2026-07-22. Sarah opens the mobile app, selects Evelyn, and taps 'Clock In'. The app captures GPS coordinates (e.g., 51.5074, -0.1278) and the timestamp. The app sends a POST request to the backend with {'carerId': 'carer-123', 'clientId': 'client-456', 'timestamp': '2024-07-22T09:00:00Z', 'latitude': 51.5074, 'longitude': -0.1278}. The backend creates a new Visit record in the database.
```

2. 2. Carer Logs Activities

```
During the visit, Sarah records activities: 'Personal Care: Assisted with dressing', 'Meals: Prepared breakfast', 'Medication Prompts: Reminded for morning meds'. She notes Evelyn's mood as 'Content' and flags 'No Concerns'. The app sends multiple POST requests to the backend with payloads like {'activityType': 'Personal Care', 'description': 'Assisted with dressing', 'timestamp': '2024-07-22T09:30:00Z'}. These create ActivityLog records linked to the Visit.
```

3. 3. Carer Clocks Out

```
At 10:00, Sarah taps 'Clock Out'. The app captures new GPS coordinates and the timestamp. It sends a POST request to the backend with {'timestamp': '2024-07-22T10:00:00Z', 'latitude': 51.5075, 'longitude': -0.1279}. The backend updates the Visit record with the clock-out time and coordinates.
```

4. 4. Wellbeing Signal Processing

```
Upon visit completion, a background process is triggered. It queries the ActivityLog records for 'client-456' for 2026-07-22. Based on rules (e.g., 'Mood: Content' + 'No Concerns' = 'Stable'), it determines Evelyn's wellbeing status for the day as 'Stable'. This updates the WellbeingSignal record for 'client-456' for 2026-07-22 to {'signal_date': '2026-07-22', 'status_level': 'Stable', 'summary_notes': 'Client was content, no concerns noted.'}.
```

5. 5. Family Member Views Dashboard

```
Evelyn's daughter, 'Maria Smith', logs into the Family Web Dashboard. The dashboard makes a GET request to the backend for client-specific information. The backend retrieves the latest Visit records and WellbeingSignal data. Maria sees a confirmation for Sarah's visit from 09:00-10:00, a summary of activities, and a 'Stable' wellbeing trend for Evelyn, with no new decline alerts.
```

7. IMPLEMENTATION PLAN

Implementation Plan

W1-W4

M1: Foundation & Carer App Core

· Project setup and environment configuration
· Core data model definition (Client, Carer, Visit)
· Carer mobile app: Login, Schedule View, Clock-in/out (GPS+Timestamp)

Exit: Carers can securely log in, view their schedule, and successfully clock in and out of visits with location data captured.

W5-W8

M2: Visit Logging & Wellbeing Rules

· Carer mobile app: Activity Logging, Mood Recording, Concern Flagging
· Backend service for processing carer observations
· Initial rule-based wellbeing signal generation logic

Exit: Carers can fully log visit details, and the backend successfully generates a daily wellbeing signal for clients based on these observations.

W9-W12

M3: Family Dashboard & Agency Scheduling

· Family web dashboard: Visit Confirmation, Wellbeing Trend Display, Basic Alerts
· Agency web portal: Carer Management, Basic Rostering & Scheduling
· Multi-tenant agency setup functionality

Exit: Family members can view visit confirmations and wellbeing trends, and agency staff can manage carers and create basic schedules for a single tenant.

W13-W16

M4: Compliance & Pilot Readiness

· Agency web portal: CQC-ready compliance reporting module
· User roles and permissions for agency staff and family members
· Security hardening and initial penetration testing

Exit: The platform supports CQC-compliant reporting, all user roles are functional, and the system is ready for a pilot launch in one region.

W17-W20

M5: Pilot Launch & Feedback

· Pilot launch support and monitoring
· User feedback collection mechanisms
· Minor bug fixes and performance optimizations

Exit: The platform is successfully deployed and in use by pilot agencies, with initial user feedback being collected and addressed.

W21-W28

M6: Scalability & Refinement

· Performance and scalability optimizations for UK-wide rollout
· Advanced security audit and compliance review (NHS DSP Toolkit)
· Refinement of wellbeing signal rules based on pilot data
· Infrastructure as Code (IaC) for multi-region deployment readiness

Exit: The platform is optimized for scale, meets full NHS DSP Toolkit standards, and is ready for broader UK rollout.

Roadmap Beyond MVP

Where this product can go after the MVP ships — the phases we'd sequence next, and the gate to enter each.

- **Phase 2**
  AI Enhancement + NHS Integration — Advanced ML/NLP models, NHS API integration, voice assistant, multi-language
- **Phase 3**
  Scale & Extend — IoT sensors, white-labelling, advanced BI, third-party integrations
- **Phase 4**
  Enterprise — Multi-region, enterprise SSO (SAML), predictive staffing, care pathway optimisation

DBBS PRE-BUILT SOLUTIONS

Modules you don't have to build

These pieces of your scope map onto modules in DBB Software's open-source platform (github.com/DBB-Software/dbbs-solutions) — production-tested in prior engagements. We do not start them from scratch; we start with a configured drop-in.

Auth + MFA + SSO
Auth0 / Cognito adapter with MFA, SSO, role-based access. Plug-and-play for B2B logins.

File Uploads + Storage
S3 / R2 / Vercel Blob uploads with on-the-fly thumbnail generation and signed URLs.

Notifications (Email + SMS + Push)
Twilio + SendGrid + push notifications with template management and delivery tracking.

Analytics + Attribution
GA4 + Mixpanel + PostHog adapter with consent-mode and server-side event proxy.

Sentry + Langfuse Observability
Pre-wired Sentry errors + Langfuse LLM traces + CloudWatch metrics. Drop-in stack.

RELEVANT WORK

Selected DBBS case studies

A selection of comparable work from our portfolio — the closest matches to your domain and build type. Full case studies on dbbsoftware.com.

RetinaRisk Case Study ’

Building a Diabetic Retinopathy Care Platform with Mobile App and Provider Portal DBB Software built a multi-surface healthcare platform for RetinaRisk. The platform helps patients track their risk of diabetic retinopathy and gives clinicians a single interface for managing patient data. About the Client RetinaRisk, an EU-based health technology company, is dedicated to preventing vision loss...

DispatchHealth onboarding platform ’

Delivering a Modern Self-Scheduling Platform for At-Home Care Find out how DBB Software helped a leading provider of in-home urgent medical care build a scalable digital self-scheduling and onboarding platform that enables patients to request care independently while reducing call-center load and improving insurance data accuracy. About the Client- DispatchHealth delivers high-quality, on-demand...

DispatchHealth migration ’

Modernizing a Healthcare Platform by Migrating a Monolith to Microservices Find out how DBB Software helped a leading U.S. at-home healthcare provider modernize its core platform by decomposing a large Ruby on Rails monolith into scalable Golang microservices, improving performance, reliability, and long-term maintainability across mission-critical patient experience flows. About the Client...

Work Breakdown & Effort Estimate

The build decomposed into workstreams, each with its key tasks and an indicative effort band — the basis for planning a budget and a delivery schedule. Effort is in person-weeks, never a price.

- **Foundations & multi-tenancy — 6–8 person-weeks**
  - – Monorepo + service scaffolding
  - – Schema-per-tenant data model + migrations
  - – RBAC core + tenant context
  - – Shared component library

  Depends on: Confirmed OQ-002, OQ-005 (tenancy model)

- **Authentication & access (Auth0) — 4–6 person-weeks**
  - – Auth0 Organizations setup + HIPAA BAA
  - – MFA + five role definitions
  - – Session + JWKS caching
  - – Invite & member management

  Depends on: Auth0 BAA timeline (OQ-010)

- **Data ingestion & provider integration — 8–10 person-weeks**
  - – Provider-abstraction interface
  - – Scheduled ingestion workers
  - – Normalisation layer + validation
  - – Admin sync-status dashboard

  Depends on: Selected data feed (OQ-006)

- **Carer mobile application — 12–16 person-weeks**
  - – Visit schedule + client list
  - – GPS + timestamp clock-in/out
  - – Activity & wellbeing logging
  - – Offline capture + sync queue
  - – Concern flagging

  Depends on: Foundations, Auth

- **Family wellbeing dashboard — 8–10 person-weeks**
  - – Visit confirmation feed
  - – Wellbeing trend views
  - – Decline alerts
  - – Consent-scoped sharing

  Depends on: Wellbeing signal

- **Agency portal & scheduling — 10–12 person-weeks**
  - – Carer rostering + availability
  - – Compliance dashboards (CQC/RQIA)
  - – Member & client management
  - – Report generation

  Depends on: Foundations, ingestion

- **Wellbeing signal & AI decline detection — 8–10 person-weeks**
  - – Rule-based scoring engine
  - – LLM-assisted decline detection (human-in-the-loop)
  - – Versioning + audit trail
  - – Clinical validation harness

  Depends on: Clinical rules (OQ-004), ingestion

- **Reporting, exports & compliance — 6–8 person-weeks**
  - – PDF / presentation report engine
  - – Org branding presets
  - – Audit logging + data-handling controls
  - – NHS DSP Toolkit alignment

  Depends on: Agency portal

- **Notifications & messaging — 4–5 person-weeks**
  - – Multi-channel dispatch (push/SMS/email)
  - – Dead-letter queue + retries
  - – Preference management

- **Observability, security & hardening — 6–8 person-weeks**
  - – OpenTelemetry + Sentry + CloudWatch
  - – Tenant-isolation penetration tests
  - – Performance tuning to SLOs
  - – DR runbook + backups

  Depends on: All feature workstreams

- **Design system & UX — 6–8 person-weeks**
  - – Design tokens + component library
  - – Carer / family / agency UX flows
  - – WCAG 2.1 AA accessibility pass
  - – Clickable prototype

  Depends on: Foundations

- **Search, filtering & profiles — 5–6 person-weeks**
  – Client/carer search + filters
  – Profile aggregation views
  – Saved views + watchlists
  Depends on: Ingestion

- **UAT, pilot onboarding & launch — 5–6 person-weeks**
  – Pilot agency onboarding
  – UAT with carer cohort
  – App-store submission
  – Go-live + monitoring
  Depends on: Hardening complete

Basis of Estimate

What the effort above is built on — the cost drivers, the estimating assumptions, and the contingency — so a budget can be planned with eyes open.

The effort bands above size the MVP scope at an Extra-Large engagement (~26 weeks, phased). They are an indicative planning basis, not a quote — a fixed bid (±15%) is produced when scope is frozen and the architecture validated.

Cost & effort drivers

· Regulated healthcare: GDPR + HIPAA + NHS DSP Toolkit + CQC/RQIA readiness raises QA, security, and audit effort
· Strict multi-tenant isolation (schema-per-tenant) across every feature
· Offline-capable mobile app with conflict resolution
· AI decline detection with human-in-the-loop validation
· Licensed data-provider integration behind an abstraction layer

Estimating assumptions

· Single licensed data provider for the MVP; second provider is Phase 2
· Responsive web + one mobile app (iOS/Android via React Native); no separate native codebases
· Pilot in one region before UK-wide scale
· Client provides clinical rules and timely UAT availability

Contingency: 10–15% contingency is recommended on top of the bands until OQ-001…OQ-010 are resolved in Discovery; the largest swing factors are the data-provider contract and the clinical validation criteria. As a three-point view: a low case of roughly 22 weeks if the provider integration is clean and clinical rules arrive early, an expected case of ~26 weeks, and a high case of ~32 weeks if a second data source or NHS accreditation is pulled into the MVP.

Delivery Plan — Sprint Schedule

The sprint-by-sprint plan we'd kick off with: each sprint a clear goal and the scope pulled into it. This is the runway from signed scope to a working product.

- **Sprint 0 (Mobilization): Team productive on day one**
  - Environments + CI/CD provisioned
  - Access + accounts granted
  - Backlog refined, DoR/DoD agreed
- **Sprint 1 — Foundations: Multi-tenant skeleton stands up**
  - Schema-per-tenant data model + migration runner
  - Tenant context + base RBAC scaffolding
  - Shared component library + design tokens
- **Sprint 2 — Authentication: Secure multi-tenant login**
  - Auth0 Organizations + HIPAA BAA wiring
  - MFA + five role definitions
  - Member invite + management; admin can log in
- **Sprint 3 — Ingestion foundations: Data lands for one region**
  - Provider-abstraction interface
  - Scheduled ingestion workers + normalisation
  - Admin sync-status dashboard
- **Sprint 4 — Data quality: Credible, validated data**
  - Validation + schema-drift tests
  - Per-league/region mapping
  - Ingestion anomaly surfacing
- **Sprint 5 — Carer app core: Carer can run a visit**
  - Schedule + client list
  - GPS + timestamp clock-in/out
  - Activity + wellbeing logging
- **Sprint 6 — Carer app resilience: Works in the field**
  - Offline capture + sync queue
  - Concern flagging
  - Conflict resolution
- **Sprint 7 — Family dashboard: Families see today's visit**
  - Visit confirmation feed
  - Consent-scoped sharing
  - Mobile-friendly views

- **Sprint 8 — Wellbeing signal: Trust the score**
  - Rule-based wellbeing scoring engine
  - Wellbeing trend views
  - Versioning + audit trail
- **Sprint 9 — Agency scheduling: Run the rota**
  - Carer rostering + availability
  - Member + client management
  - Scheduling conflict checks
- **Sprint 10 — Compliance & reporting: Inspection-ready**
  - CQC/RQIA compliance dashboards
  - PDF / presentation report engine
  - Org branding presets
- **Sprint 11 — AI decline detection: AI assists, humans decide**
  - LLM-assisted decline detection (human-in-the-loop)
  - Clinical validation harness
  - Fallback to rule-based
- **Sprint 12 — Notifications: The right alert reaches the right person**
  - Multi-channel dispatch (push/SMS/email)
  - Dead-letter queue + retries
  - Preference management
- **Sprint 13 — Hardening & launch: Pilot-ready**
  - Security + tenant-isolation penetration tests
  - Performance tuning to SLOs
  - UAT sign-off; app-store submission; go-live

Mobilization — Sprint 0

The setup work that happens before feature delivery so the team is productive from day one of Sprint 1.

A focused Sprint 0 stands up the delivery rails so feature work starts immediately in Sprint 1: cloud environments, pipelines, access, and an agreed way of working.

Environments

- AWS eu-west-1 dev / staging / production (Terraform-provisioned)
- Per-tenant schema isolation enabled from day one
- Seeded synthetic (non-PHI) test data

CI/CD & tooling

- GitHub Actions pipelines (lint, test, type-check, deploy)
- Infrastructure-as-code (Terraform) reviewed + applied
- Preview deployments per pull request

Access & accounts

- AWS accounts + least-privilege IAM roles
- Auth0 tenant + HIPAA BAA initiated
- Repository, Jira, Slack, Figma access for both teams

Kickoff checklist

- Open questions OQ-001…OQ-010 owners + dates confirmed
- Definition of Ready / Done agreed
- Sprint cadence + ceremony calendar set
- Risk register reviewed with the client
- Compliance contacts (CQC/RQIA, DPO) identified

RACI Matrix

Who is Responsible, Accountable, Consulted, and Informed for each delivery activity — so ownership is unambiguous from kickoff.

- **Architecture & ADR decisions**
  R: Tech Lead / Architect · A: Tech Lead / Architect · C: Client Product Owner · I: Delivery team
- **Sprint delivery**
  R: DBB engineers · A: Project Manager · C: Product Owner · I: Stakeholders
- **Code review & quality**
  R: DBB engineers · A: Tech Lead · C: — · I: PM
- **UAT & acceptance sign-off**
  R: Client Product Owner · A: Client Product Owner · C: QA Engineer · I: DBB team
- **Compliance approval (CQC/RQIA, GDPR/HIPAA)**
  R: Client + DPO · A: Client Product Owner · C: Tech Lead · I: Delivery team
- **Release & go-live**
  R: DevOps Engineer · A: Project Manager · C: Tech Lead · I: Client
- **Change requests**
  R: Project Manager · A: Product Owner · C: Tech Lead · I: Delivery team
- **Data / PHI governance**
  R: Tech Lead · A: Client DPO · C: Security · I: All
- **Backlog prioritisation**
  R: Product Owner · A: Product Owner · C: Tech Lead + PM · I: Delivery team
- **Security & penetration testing**
  R: DBB engineers + QA · A: Tech Lead · C: Client DPO · I: PM
- **Infrastructure & environments**
  R: DevOps Engineer · A: Tech Lead · C: Client IT · I: Delivery team
- **Stakeholder communication**
  R: Project Manager · A: Project Manager · C: Product Owner · I: All stakeholders

Definition of Done & Governance

The quality bar every increment is held to, how work is accepted and signed off, and how change is controlled once the build is underway.

Definition of Done

- Code reviewed, merged, and deployed to staging
- Automated unit + integration tests passing; coverage maintained
- Acceptance criteria demonstrably met
- Accessibility (WCAG 2.1 AA) checked for user-facing work
- No new critical/high security findings; PHI never logged
- Documentation + ADRs updated where decisions changed
- Observability in place (logs, metrics, alerts) for new surfaces
- Performance within agreed SLOs for the touched paths
- Product Owner has accepted the story in the sprint demo

Acceptance & sign-off: Each sprint ends in a demo against the sprint goal; the Product Owner accepts stories whose acceptance criteria are met. A milestone is signed off when its exit criteria pass and UAT is approved.

Change control: Scope changes are raised as change requests through the PM, sized in person-weeks against the work breakdown, and accepted or deferred by the Product Owner before they enter a sprint — the fixed scope in this document is the baseline.

8. TEAM COMPOSITION

Team Composition

The DBBS team that ships this project on your behalf — end-to-end. Not staff augmentation of your engineers.

Product Manager

×1 FTE

Defines product vision, manages roadmap, gathers requirements, and ensures alignment with business goals and user needs.

Technical Lead

×1 FTE

Oversees technical architecture, guides engineering decisions, ensures code quality, and mentors the development team.

Frontend Engineer

×2 FTE

Develops the Carer Mobile App (React Native) and the Family/Agency Web Dashboards (Next.js), ensuring responsive and intuitive user interfaces.

Backend Engineer

×2 FTE

Builds the core API services, manages database interactions, implements business logic, and develops the wellbeing signal processing engine.

DevOps / Platform Engineer

×1 FTE

Manages cloud infrastructure (AWS), implements CI/CD pipelines, ensures system scalability, reliability, and observability.

QA Engineer

×1 FTE

Designs and executes test plans, performs functional, integration, performance, and security testing, and ensures overall product quality and compliance.

Compliance & Security Specialist

×0.5 FTE

Advises on UK GDPR, NHS DSP Toolkit, and CQC compliance, reviews security practices, and ensures data protection standards are met.

9. RISK ASSESSMENT

Risk Assessment & Mitigations

RISK	IMPACT	MITIGATION
Auth0 outage blocks all authentication	HIGH	Cache JWKS locally. Circuit breaker with graceful degradation (read-only mode). Auth0 enterprise SLA: 99.99%
Schema-per-tenant migration failures at scale (>50 tenants)	HIGH	Automated migration runner with per-tenant rollback. Blue-green schema migration strategy
LLM agent produces inaccurate decline assessments	HIGH	Rule-based scoring provides deterministic baseline. LLM agent outputs always require human review. Circuit breaker falls back to rule-based only if LLM is unavailable
Offline sync conflicts in mobile app	MEDIUM	Last-write-wins with conflict detection. Server-side conflict queue for manual resolution
Background GPS tracking causes excessive battery drain	MEDIUM	GPS active only during check-in/out. Significant location change API (iOS) / fused provider (Android)
PostgreSQL connection pool exhaustion	HIGH	PgBouncer sidecar. Connection alerts at 80%. Read replicas offload analytical queries
Bull/Redis queue failure causes notification loss	HIGH	Redis AOF persistence. Dead letter queue. Multi-channel fallback (push -> SMS -> email)
React Native Expo limitations require native module	MEDIUM	Expo development builds support native modules without full eject
App store rejection delays mobile go-live	HIGH	Pre-submission compliance checklist. TestFlight / internal testing. Buffer: 1-2 weeks
Scope creep from client's broader product vision	MEDIUM	MVP scope defined in SDD. Change request process via PM. Post-MVP documented separately
HIPAA BAA negotiation with Auth0 delays start	HIGH	Initiate early (Sprint 0). Fallback: AWS Cognito as interim auth
Client team unfamiliar with agile delivery	MEDIUM	PM-led onboarding. Clear RACI matrix. Regular demos and feedback loops
Multi-language requests during MVP	LOW	Documented as Phase 2. i18n infrastructure set up in MVP to minimise future effort
Care agencies reluctant to adopt new platform	HIGH	Pilot with interested agencies. Simple onboarding. Mobile-first UX for non-technical carers

Regulatory changes (CQC/RQIA)	HIGH	Configurable compliance rules. Modular compliance module updated independently
NHS API integration requires accreditation/fees	MEDIUM	NHS APIs deferred to Phase 2. Manual data entry in MVP. Accreditation fees flagged as OQ
GDPR erasure request for regulatory-retained data	HIGH	Pseudonymisation instead of deletion. Manager approval for active care data erasure
Competitor adds family portal or AI features	MEDIUM	First-mover in combined care + AI + community. Continued AI investment
Data breach during pilot	HIGH	Defence-in-depth (3-layer isolation, encryption, WAF, audit). Incident response plan

AI Opportunities

Where applied AI/ML adds defensible value to this product — built responsibly, with provider abstraction, fallbacks, and human-in-the-loop where it matters.

- **Rule-Based Wellbeing Signal (MVP)**

  Automate the generation of a client wellbeing status based on carer observations, providing immediate value to family dashboards.

  Approach: Implement a configurable rule engine that processes structured carer input (mood, activity, flagged concerns) to derive a composite wellbeing score or status. This forms the foundation for future AI enhancements.

- **LLM-Assisted Decline Detection (Post-MVP)**

  Analyze free-text carer notes and structured observations to detect subtle patterns indicative of client decline, beyond simple rule thresholds.

  Approach: Develop a pipeline that feeds anonymized carer notes and structured data into a fine-tuned LLM. The LLM would identify nuanced changes in behavior or health, flagging potential decline for agency review. This requires a human-in-the-loop validation process to ensure accuracy and prevent 'hallucinations'.

- **Carer Observation Summarization (Post-MVP)**

  Automatically summarize daily or weekly carer observations for family members and agency staff, reducing reading time and highlighting key points.

  Approach: Utilize an LLM to generate concise summaries of carer visit notes, focusing on key activities, mood changes, and flagged concerns. Summaries would be reviewed for accuracy before presentation to users.

10. DEVELOPMENT PROCESS

Development Process

Cadence

Two-week sprints

Ceremonies

- Sprint Planning
- Daily Stand-ups
- Sprint Review
- Sprint Retrospective

Tooling

GitHub for version control · Jira for project management · Slack for team communication · Confluence for documentation

Support & Maintenance

Post-launch, DBBS offers a tiered support and maintenance agreement, providing ongoing operational stability and continuous improvement.

Service levels: Critical (P1) issues: 1-hour response, 4-hour resolution target. High (P2) issues: 2-hour response, 8-hour resolution target. Medium (P3) issues: 4-hour response, 24-hour resolution target. Low (P4) issues: 8-hour response, 48-hour resolution target.

- 24/7 monitoring of critical systems and infrastructure
- Bug fixes and security patches
- Performance optimization and scalability management
- Minor feature enhancements and platform updates
- Dedicated support channel for incident reporting

Testing & QA Strategy

A 'shift-left' testing approach will be adopted, integrating testing throughout the development lifecycle. This includes automated tests at multiple levels and manual testing for critical user flows and compliance verification.

- Unit Testing (for individual functions and components)
- Integration Testing (for API endpoints and service interactions)
- End-to-End Testing (for critical user journeys across mobile and web platforms)
- Performance Testing (to ensure scalability and responsiveness)
- Security Testing (including penetration tests and vulnerability scans)
- User Acceptance Testing (UAT) with Caraway Care staff and pilot users

Data Strategy & AI-Readiness

The data strategy prioritizes security, privacy, and compliance with UK GDPR and NHS DSP Toolkit standards. All data will be stored in PostgreSQL with a multi-schema approach for tenant isolation. Strict access controls (RBAC) will govern who can view and modify PHI. Data quality will be maintained through input validation in the carer app and agency portal.

- Data ownership for each agency tenant will be clearly defined, with DBBS acting as a data processor.
- Anonymization and pseudonymization techniques will be applied for any data used in analytics or future AI model training.
- Data retention policies will be enforced automatically based on regulatory requirements and client agreements.
- Audit trails for all PHI access and modification will be maintained for compliance purposes.
- A data governance framework will be established to manage data definitions, quality, and lifecycle.

OVERALL EFFORT

Start lean: ~16 weeks · Full rollout: ~28 weeks

Full build sizing: Extra Large — 6+ months

WHAT OUR CLIENTS SAY

“They provided quality healthcare CRM software with great support, making the experience enjoyable.”

Linda William · Technical Operations Manager at Blue Medi Home Health Care Center

Standards & Best Practices

This Scoping Sprint deliverable is structured to the recognised software-engineering standards a senior team uses, so a reviewing engineer can navigate and trust it like any hand-authored design document. We follow the principles of these frameworks — we do not claim formal certification against them (most are not certifications). The one held certification, ISO/IEC 27001, is DBB Software's as an organisation.

arc42 — architecture documentation

The document's flow — project context and goals, scope, constraints and assumptions, the proposed technical solution, quality attributes, and risks — follows the arc42 architecture-documentation template. arc42 is a template, not a certification.

ISO/IEC/IEEE 29148 — requirements engineering

Requirements follow this standard's principles: functional requirements are individually stated, each carries a priority, and each is paired with testable acceptance criteria; scope is split into in-scope, out-of-scope, and measurable success metrics; non-functional requirements are a distinct set alongside ranked quality attributes.

MoSCoW prioritisation (three-band)

Every functional requirement carries an explicit P0/P1/P2 priority mapping to Must / Should / Could, separating the committed core from negotiable scope. It is a three-band application (no 'Won't' band); deliberately excluded items live in the out-of-scope section.

The C4 model (Simon Brown) — architecture diagrams

The architecture is shown as a C4-style system view, with a data-flow diagram and sequence diagrams, describing structure and runtime behaviour at consistent abstraction levels. Sequence diagrams are a recognised C4 dynamic supplement; the data-flow diagram is a complementary view, not itself a C4 diagram type.

Architecture Decision Records (Michael Nygard)

Significant technical choices are captured as ADRs — context, decision, and consequences — alongside a technology-evaluation table and an entity-relationship data model, so each recommendation is traceable to a stated rationale and its trade-offs rather than asserted.

IEEE 1016 — Software Design Description

The proposed-solution chapter is organised in the spirit of an IEEE 1016 design description — architecture overview, recommended stack, data model, ADRs, and a rendered diagram set — sized to a scope document, not a full IEEE 1016 specification with formal viewpoint coverage.

ISO/IEC 27001 — information security (DBB Software is certified)

DBB Software holds ISO/IEC 27001 certification for its information-security management system — the one formal, audited certification here, and a property of DBB the organisation, NOT of this document. Separately, the document includes a data-handling table (data class, lawful basis, retention, residency) reflecting GDPR-style data governance.

Senior-architect & engineering review

This deliverable is authored and reviewed by a senior DBBS architect with the engineering team, not generated — every recommendation is a considered judgement validated against our delivery experience, and the scope, estimate, and architecture are signed off before it reaches you.

PMI Work Breakdown Structure & delivery governance

This document includes a PMI-style Work Breakdown Structure with effort bands, a basis-of-estimate (cost drivers, assumptions, contingency, and a three-point range), a sprint-by-sprint delivery plan, a Sprint-0 mobilisation plan, a RACI matrix, a Definition of Done, and a change-control process. The WBS draws on PMI practice; RACI, the Definition of Done, and change control are general delivery-governance artefacts.

In plain terms: the structure follows the principles of arc42, ISO/IEC/IEEE 29148, the C4 model, IEEE 1016, MoSCoW, ADRs, and PMI / agile delivery practice — none of which are certifications. ISO/IEC 27001 is the single held certification, and it belongs to DBB Software.

11. NEXT STEPS

Next Steps

1. Schedule a 30-minute Discovery call to confirm assumptions and refine the project scope.
2. Conduct a Build Readiness Diagnostic to assess current infrastructure, data, and team capabilities.
3. Initiate a fixed-bid Scoping Sprint to produce detailed user stories, technical specifications, and a precise project plan.
4. Kick off the MVP build with a dedicated DBBS team, delivering the core platform features.

IF YOU TAKE THE NEXT STEP

What DBBS Discovery produces

- A refined technical architecture validated against your constraints — not invented from a chat.
- UX wireframes for the core flows, signed off by your team.
- A frozen scope: every functional requirement explicitly in or out.
- A fixed-price quote for the MVP build, with milestones and dependencies mapped.
- A team composition + onboarding plan ready to start the build the day Discovery closes.

On budget: we don't quote from a single chat. An indicative, phase-by-phase range — and the fixed-price MVP quote — come out of the Discovery phase above, once the scope is frozen and the architecture validated.

DBB Software is ISO/IEC 27001 certified. Your data, source code, and IP are handled under an independently audited information-security management system.

HOW THIS SCOPE WAS PRODUCED

This is an illustrative **DBBS Scoping Sprint** deliverable — produced by a senior architect with our engineering team and grounded in our delivery experience. A Sprint for your project turns your idea into exactly this: a validated, build-ready scope, UI wireframes, and a fixed-price Statement of Work — with the fee credited against the build.

Start DBBS Product Discovery ->

SCAN OR CLICK TO BOOK