

Architecture — Component HLD Master

LumisCare — Component High-Level Design Master Document

Version: 1.0 **Date:** 2026-04-04 **Author:** Dr. Sarah Chen, Healthcare IT Systems Architect **Status:** Active — Reflects verified implementation state as of 2026-04-04 **Method:** Static analysis of source tree + HLD document review + gap analysis synthesis

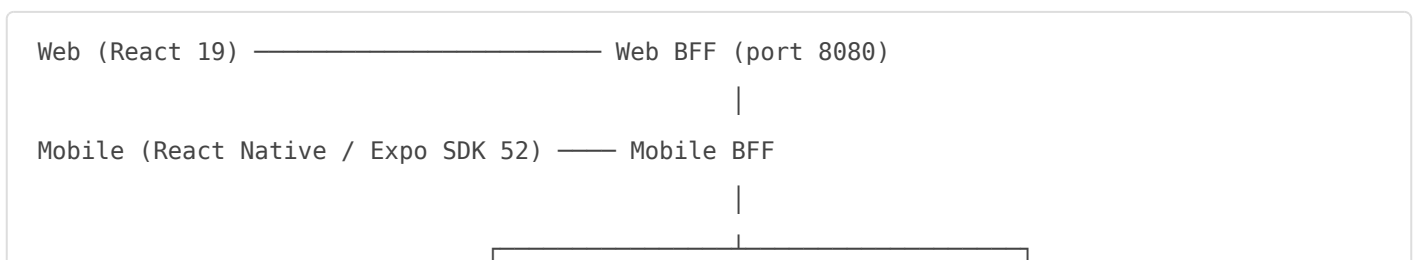
Document Purpose

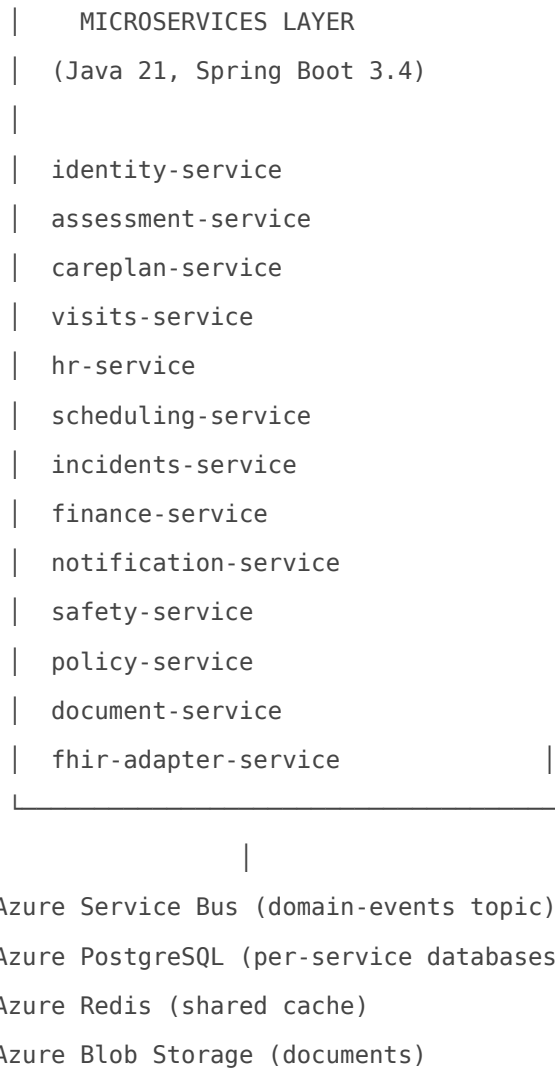
This document provides the authoritative component-level HLD for all LumisCare microservices, BFF layers, and frontend features. It cross-references the documented architecture (VCC2-C4-Architecture-Diagrams.md, Services-Integration-Matrix.md, BFF-Architecture-Design.md, Service-Bus-Subscriptions-Design.md) against verified implementation on disk.

Each component section records: implementation status, controller/entity counts, BFF integration status, event bus wiring status, and known gaps.

CRITICAL NOTE — Naming inconsistency: HLD documents use "VCC 2.0" throughout. The BFF design switches to "iCON". The deployed product is "LumisCare". All three names refer to the same system. This document uses "LumisCare" as the canonical product name.

System Architecture Summary





Multi-tenancy: Row-Level Security (RLS) on `organisation_id` across all service databases. **Auth:** Azure Entra ID (MSAL) — JWT pass-through from BFF to microservices. Service-to-service via Azure Managed Identity. **Deployment:** Azure Container Apps (AKS target). Azure Static Web Apps for frontend.

Component Status Legend

Status	Meaning
PRODUCTION-READY	Controllers, entities, repositories, and migrations all present and verified
PARTIAL	Core entities and controllers present but key integration (event bus, BFF, mobile) absent
SKELETON	Directory exists, minimal or no Java source files
UNDOCUMENTED	Implemented in code but absent from all HLD documents
DESIGN-ONLY	Documented in HLD but not implemented in code

Component Index

1. Identity
 2. HR
 3. Visits
 4. Scheduling
 5. Care Plans
 6. Assessments
 7. Incidents
 8. Finance
 9. Notifications
 10. Safety
 11. Policy (AI/RAG)
 12. Document
 13. FHIR Adapter
 14. Web BFF
 15. Mobile BFF
-

1. Identity

Purpose

Manages users, organisations, service users, RBAC roles, consent records, PHI access audit, and GDPR data rights. Serves as the authentication enrichment layer for Azure Entra ID tokens — all services call identity-service to resolve user context from JWTs.

Backend Service

- **Status:** PRODUCTION-READY
- **Controllers:** 8 — ConsentController, OrganizationController, ServiceUserController, RoleController, AuthInternalController, DataRightsController, SafetyController, UserController
- **Entities:** 11 — UserEntity, ServiceUserEntity, RoleEntity, OrganizationEntity, ConsentEntity, EmergencyContactEntity, OrganizationSettingsEntity, PhiAccessAuditEntity, PhiAnomalyAlertEntity, DataRightsRequestEntity, DnacprAuditLogEntity
- **Repositories:** 10 — UserRepository, ServiceUserRepository, RoleRepository, OrganizationRepository, ConsentRepository, EmergencyContactRepository, PhiAccessAuditRepository, PhiAnomalyAlertRepository, DataRightsRequestRepository,

DnacprAuditLogRepository

- **Migrations:** 14 Flyway migrations (V8: role permissions, V12: PHI access audit and anomaly tables)
- **Key capabilities:**
 - Multi-tenant organisation isolation via RLS on organisation_id
 - PHI access audit infrastructure (PhiAccessAuditEntity, PhiAnomalyAlertEntity) — HIPAA minimum-necessary enforcement at data layer
 - DNACPR audit log repository (DnacprAuditLogEntity) — advance directive capture. NOTE: creates dual-domain ownership with assessment-service (see Gaps)
 - DataRightsController — GDPR/UK GDPR data subject access request workflow
 - ConsentController + ConsentEntity — consent lifecycle management
 - AuthInternalController — Entra ID token enrichment (JWT → VCC claims)
 - RoleController — RBAC role and permission management

Frontend

- **Pages:** /admin/users, /admin/roles, auth pages (login, MFA, OTP)
- **Status:** Real — users, roles, and auth pages implemented in src/features/admin/users, src/features/admin/roles, src/features/admin/organizations

BFF Integration

- **web-bff:** UsersController, OrganizationsController — GET /users/{id}, GET /organizations/{id}, GET /service-users/{id}
- **mobile-bff:** No dedicated controller confirmed — identity resolution happens via JWT enrichment on every request

Event Bus

- **Publishes:** No event publisher confirmed in source
- **Subscribes:** Consumes employee.created and employee.terminated from HR (documented in Integration Matrix; HrEventPublisher exists in hr-service)
- **Status:** NOT WIRED — no identity-service event publisher found; subscription to HR events not confirmed in source despite being documented

Gaps

- No event publisher — service user onboarding events (serviceuser.created) are not published, preventing other services from reacting to new intake
- DNACPR dual-domain ownership: DnacprAuditLogEntity in identity-service and DnacprOrderEntity in assessment-service have no confirmed synchronisation mechanism. For a resuscitation decision, this is clinically unacceptable — a DNACPR order cancelled in assessment-service may not be reflected in the identity audit log

- No confirmed break-glass emergency access pattern implementation (entity infrastructure exists but controller-level break-glass with audit is not confirmed)
 - No event publisher means identity cannot signal account deactivation to scheduling-service for orphan appointment cleanup
-

2. HR

Purpose

Manages employee records, qualifications, training certifications, availability preferences, leave management, performance reviews, and equality/diversity data. Acts as the canonical source of carer workforce data for the scheduling-service.

Backend Service

- **Status:** PRODUCTION-READY
- **Controllers:** 12 — EmployeeController, EmployeeSearchController, EmployeeNoteController, AvailabilityPreferencesController, TrainingRecordController, TrainingCertificateUploadController, EducationTrainingController, PerformanceReviewController, LeaveManagementController, SupportingDocumentController, HealthInformationController, ClientFeedbackController
- **Entities:** 12+ — EmploymentHistory, PerformanceReview, LeaveRecord, TrainingRecord, EducationTraining, CertificateUploadTracking, ResumeUploadTracking, HealthInformation, EqualityDiversity, NextOfKin, EmployeeReference, AvailabilityPreferences
- **Repositories:** 12 — EmployeeRepository, LeaveRecordRepository, PerformanceReviewRepository, TrainingRecordRepository, EducationTrainingRepository, AvailabilityPreferencesRepository, CertificateUploadTrackingRepository, ResumeUploadTrackingRepository, HealthInformationRepository, ClientFeedbackRepository, EmployeeReferenceRepository, SupportingDocumentRepository
- **Migrations:** 24 Flyway migrations (highest in the fleet — V14: leave records, V15: performance reviews)
- **Key capabilities:**
 - HealthInformation as separate entity — appropriate PHI boundary for staff health data
 - CertificationExpiryScheduler — scheduled job for expired training certificate detection (CQC Regulation 17 compliance)
 - HrEventPublisher — publishes HR events to Azure Service Bus
 - AvailabilityPreferencesService — publishes availability changes consumed by scheduling-service
 - LeaveManagementService — publishes leave approval events

- Bradford Factor calculation support

Frontend

- **Pages:** `/employees` (list), `/employees/:id` (detail), HR sub-pages for DBS, Training, Bradford Factor, Supervisions
- **Feature directory:** `src/features/backOffice/hr/`
- **Status:** Real — hr feature has full component structure (api, components, constants, hooks, models, pages, schemas, services, store, utils)

BFF Integration

- **web-bff:** `EmployeeController`, `HrComplianceController`, `ResumeUploadController` — GET `/employees`, GET `/employees/{id}/availability`, GET `/employees/{id}/compliance`
- **mobile-bff:** No dedicated HR controller — carer profile accessed via `CarerScheduleController`

Event Bus

- **Publishes:** `employee.created`, `employee.terminated`, `availability.updated`, `leave.approved`, `skill.added`
- **Subscribes:** Nothing confirmed (HR is primarily a publisher; scheduling-service consumes its events)
- **Status:** WIRED — `HrEventPublisher`, `AvailabilityPreferencesService`, `LeaveManagementService` all confirmed in source. `AvailabilityUpdatedEventListener` confirmed in scheduling-service as consumer.

Gaps

- Entity naming inconsistency: HR entities do not use the `*Entity.java` suffix convention used by other services. This does not affect runtime but complicates static analysis tooling and cross-service code navigation
- `ClientFeedbackController` sits in hr-service — client feedback data may belong in assessment-service or incidents-service by domain
- No BFF controller for employee DBS (Disclosure and Barring Service) record status — DBS expiry is a CQC compliance item and should be surfaced to care coordinators via a dedicated endpoint

3. Visits

Purpose

Manages the full visit execution lifecycle: Electronic Visit Verification (EVV) check-in/check-out, care note recording, eMAR (electronic medication administration record), vital sign capture, task completion, observation recording, real-time carer location tracking, and geofence enforcement. The most clinically active service during field operations.

Backend Service

- **Status:** PRODUCTION-READY
- **Controllers:** 12 — VisitController, VisitLifecycleController, EVVController, EmarController, MedicationController, MedicationRefusalController, TaskController, ObservationController, VitalSignController, CareNoteController, GeofenceController, TrackingController
- **Entities:** 13+ — EVVRecord, EmarRecord, MedicationSchedule, MedicationAdministration, VisitTask, VitalSignRecord, TrackingSession, Geofence, Observation, ObservationThreshold, ObservationType, TaskStatus, MedicationRefusalAlert
- **Repositories:** 12 — VisitRepository, EVVRecordRepository, EmarRecordRepository, MedicationScheduleRepository, MedicationAdministrationRepository, MedicationRefusalAlertRepository, VitalSignRecordRepository, CareNoteRepository, CarerLocationRepository, TrackingSessionRepository, VisitTaskRepository, ObservationRepository
- **Migrations:** 7 Flyway migrations (V9: observation threshold table, V13: PRN minimum interval hours)
- **Key capabilities:**
 - EVV 6-data-element compliance (21st Century Cures Act): service type, carer ID, service user ID + Medicaid ID, start/end GPS coordinates, transmission status with timestamp, manual override with reason
 - TransmissionStatus enum (PENDING/TRANSMITTED) with EVVService aggregator submission pipeline
 - MedicationAdministration with requiresWitness, witnessedBy, witnessSignatureUrl — controlled substance double-check protocol at entity level
 - V13 migration: prn_min_interval_hours — PRN medication safety interval enforcement
 - MedicationRefusalController + MedicationRefusalAlertRepository — refusal recording and alerting
 - GeofenceController — service user address boundary enforcement
 - TrackingController — real-time carer location (30-second intervals to Redis + Azure Web PubSub for dashboard)

Frontend

- **Pages:** `/visits` (list), `/visits/:id` (detail), live tracking dashboard, geofence configuration, visit handoff

- **Feature directory:** `src/features/backOffice/visits/` with subdirectories: api, components, geofence, handoff, hooks, liveTracking, pages, services, store, types, utils
- **EVV feature:** `src/features/backOffice/evv/` — EVVPage, EVVComplianceReport, EVVRecordsList, EVVManualCheckInForm, EVVRecordDetail, EVVFilters
- **Status:** Real — full component structure confirmed

BFF Integration

- **web-bff:** VisitsController, HandoffController, CompletedEventsController — GET /visits, GET /visits/{id}/full-details (aggregates visit + care plan tasks + service user + carer), GET /completed-events
- **mobile-bff:** CarerScheduleController (MobileVisitsClient) — GET /my-visits/today, POST /visits/{id}/check-in, POST /visits/{id}/check-out, POST /visits/{id}/tasks/{taskId}/complete, POST /tracking/location
- **CRITICAL GAP:** Mobile BFF has no eMAR controller, no EVV dedicated controller, no vital signs controller, and no care note controller. If mobile carers access these endpoints, they bypass the BFF layer entirely.

Event Bus

- **Publishes:** `visit.checkedin`, `visit.completed`, `task.flagged`, `checkin.timeout`, `assistance.requested`, `location.updated`, `redflag.detected` (VisitEventPublisher confirmed in source)
- **Subscribes:** No subscription confirmed (documented as publisher-only in MVP Integration Matrix)
- **Status:** PARTIALLY WIRED — VisitEventPublisher exists; however, no consumer-side listeners confirmed in finance-service for `visit.completed` (the event that should trigger invoice line item creation)

Gaps

- Only 7 Flyway migrations for a service with 12 controllers and significant clinical data scope — schema change audit trail is incomplete; later entity changes may have been applied via ORM DDL rather than versioned migrations (compliance risk for schema change governance)
- No confirmed barcode/NFC medication verification integration at the EmarController layer — entity exists but scan endpoint not confirmed
- Mobile BFF missing: eMAR recording, EVV check-in/check-out (dedicated), vital sign capture, incident reporting, and SOS — if mobile app calls these directly (bypassing BFF), JWT scope enforcement, PHI boundary logging, and API gateway rate limiting are not applied consistently (HIPAA minimum-necessary enforcement gap)
- Controlled substance witness enforcement: MedicationAdministration has the correct entity fields (requiresWitness, witnessedBy, witnessSignatureUrl) but business logic enforcement preventing "given" status without a witness signature needs to be confirmed

- at EmarController service layer — entity-level fields are necessary but not sufficient
 - Finance-service has no confirmed listener for `visit.completed` event — invoicing cannot be triggered automatically from visit completion
-

4. Scheduling

Purpose

Creates, manages, and publishes care schedules. Handles recurring appointment generation, carer assignment with skill matching, schedule approval workflow, cover arrangements, and proposed appointment review. Bridges care plan proposed visits and operational visit execution.

Backend Service

- **Status:** PRODUCTION-READY
- **Controllers:** 9 — AppointmentController, RecurringScheduleController, ScheduleController, ScheduleApprovalController, ScheduleAlertController, ScheduleEventController, CoverController, ProposedAppointmentReviewController, FinanceController
- **Entities:** 7 — AppointmentEntity, RecurringScheduleEntity, ScheduleGenerationEntity, ScheduleAlertEntity, ScheduleEventEntity, CarePlanEventIdempotencyEntity, HrAvailabilityEventIdempotencyEntity
- **Repositories:** 7 — AppointmentRepository, RecurringScheduleRepository, ScheduleGenerationRepository, ScheduleAlertRepository, ScheduleEventRepository, CarePlanEventIdempotencyRepository, HrAvailabilityEventIdempotencyRepository
- **Migrations:** 13 Flyway migrations (V9: travel time on appointments, V13: rejected status on schedule generations)
- **Key capabilities:**
 - Two-step scheduling governance: ScheduleApprovalController + ProposedAppointmentReviewController
 - Idempotency repositories (CarePlanEventIdempotency, HrAvailabilityEventIdempotency) — duplicate event delivery from care plan or HR will not create duplicate appointments
 - AppointmentEventPublisher — outbound event publishing for schedule lifecycle events
 - HrAvailabilityUpdatedEventHandler — consumes HR events to keep schedules consistent with carer availability
 - FinanceController within scheduling-service — feeds billable hours data to finance-service
 - Travel time field (V9 migration) — routing time included in appointment planning

- ScheduleAlertController + ScheduleAlertEntity — alert generation for scheduling conflicts

Frontend

- **Pages:** `/scheduling` (week/month view), appointment detail, cover requests, schedule approval workflow
- **Feature directory:** `src/features/backOffice/scheduling/` with subdirectories: components, pages, services, types
- **Status:** Real — confirmed component structure

BFF Integration

- **web-bff:** SchedulingController, CalendarController — GET `/schedules`, POST `/schedules`, PUT `/schedules/{id}/publish`, GET `/calendar` (aggregated view)
- **mobile-bff:** AppointmentsController (AppointmentsService via scheduling-service) — GET `/my-appointments`, GET `/appointments/{id}`

Event Bus

- **Publishes:** `schedule.published`, `schedule.updated` (AppointmentEventPublisher confirmed)
- **Subscribes:** `availability.updated`, `leave.approved` from hr-events (HrAvailabilityUpdatedEventHandler confirmed with idempotency); `careplan.published` from careplan-events (CarePlanEventIdempotencyEntity present — idempotency ready, but no publisher on careplan-service side)
- **Status:** PARTIALLY WIRED — publisher confirmed; HR subscription confirmed (fully wired); careplan.published subscription is idempotency-ready but the publisher (careplan-service) does not exist

Gaps

- ScheduleAlertEntity has AlertType and AlertSeverity enums but no confirmed integration path to notification-service for alert delivery — scheduling alerts may not reach care managers
 - Travel time (V9 migration) is stored but no routing API integration confirmed — travel time is entered manually, not calculated from a routing service
 - CarePlanEventIdempotencyEntity exists and is ready to consume careplan.published — but the careplan-service has no event publisher, so this idempotency infrastructure is currently unused
 - No confirmed mobile BFF endpoint for cover requests or schedule change notifications to carers
-

5. Care Plans

Purpose

Manages the full care plan lifecycle: AI-assisted generation from assessments, plan versioning, task definition, master visit type configuration, and proposed visit generation. The care plan is the primary clinical document linking assessment outcomes to scheduled care delivery.

Backend Service

- **Status:** PRODUCTION-READY
- **Controllers:** 5 — CarePlanController, AiGenerationController, MasterTaskController, MasterVisitTypeController, CarePlanVersionHistoryController
- **Entities:** 8 — CarePlan, CarePlanVersion, MasterVisitType, MasterTaskType, MasterTaskCategory, TaskDefinition, ProposedVisit, AiMetrics
- **Repositories:** 8 — CarePlanRepository, CarePlanVersionRepository, MasterVisitTypeRepository, MasterTaskCategoryRepository, MasterTaskRepository, TaskDefinitionRepository, ProposedVisitRepository, AiMetricsRepository
- **Migrations:** 10 Flyway migrations (V2: care plan version table, V4: master task type table)
- **Key capabilities:**
 - Care plan versioning: CarePlanVersion entity + CarePlanVersionHistoryController — full version history with diff capability
 - Approval-to-publish workflow: CarePlan has status, publishedAt, publishedBy fields
 - AI-assisted care plan generation: AiGenerationController + AiMetricsRepository — instrumented for outcome tracking
 - ProposedVisit entity — proposed visit schedule generated from care plan tasks, consumed by scheduling-service
 - MasterVisitType and MasterTaskType — configurable task library per organisation

Frontend

- **Pages:** `/carePlans` (list), `/carePlans/:id` (detail with version history), AI care plan generator (`/ai/care-plan-generator`)
- **Feature directory:** `src/features/backOffice/carePlans/` (components, pages, services), `src/features/backOffice/ai/AICarePlanGeneratorPage.tsx`
- **Status:** Real — confirmed component structure

BFF Integration

- **web-bff:** CarePlanController (BFF) — GET `/care-plans/{id}`, POST `/care-plans/generate`, GET `/care-plans/{id}/version-history`

- **mobile-bff:** CarePlanController (mobile) — GET /care-plans/{id} (read-only, for visit execution context)
- **Generated client:** assessment-client and careplan-client are generated OpenAPI clients in both BFFs

Event Bus

- **Publishes:** `careplan.published`, `careplan.updated` — DOCUMENTED in C4 diagram and Integration Matrix but NO event publisher class found in careplan-service source
- **Subscribes:** `assessment.completed` — DOCUMENTED as trigger for AI generation but NO subscription listener found in careplan-service source
- **Status:** NOT WIRED — neither publisher nor subscriber is implemented. This is the most critical clinical workflow gap in the platform: the Assessment → Care Plan → Schedule chain has broken links at both ends of careplan-service

Gaps

- No event publisher for `careplan.published` — scheduling-service cannot pick up a newly published care plan automatically (CarePlanEventIdempotencyEntity in scheduling-service is ready but has no events to consume)
- No subscription listener for `assessment.completed` — AI care plan generation must be triggered manually rather than automatically on assessment completion
- No RiskAssessment entity within careplan-service — risk assessments are in assessment-service (appropriate) but linkage/reference between care plan and risk assessment outcomes is not confirmed
- No countersignature or RN approval workflow entity visible at care plan level (publishedBy exists but role constraint enforcement at controller level not confirmed)
- AiMetrics entity tracks generation but no confirmed outcome feedback loop (care plan quality improvement over time requires feedback from visit task completion data)

6. Assessments

Purpose

Manages the complete clinical assessment lifecycle: intake, section/question/answer management, risk assessments (NEWS2, Waterlow, PHQ-9, GAD-7), Mental Capacity Assessment (MCA), DNACPR order management, medication reconciliation, clinical scoring, AI-assisted assessment transcription, and real-time collaborative assessment via Azure Web PubSub.

Backend Service

- **Status:** PRODUCTION-READY — highest controller count in the fleet
- **Controllers:** 23 — AssessmentIntakeApiController, AssessmentStatusApiController, AssessmentQuestionsApiController, AssessmentAnswersApiController, AssessmentSectionsApiController, AssessmentSubsectionsApiController, AssessmentMembersApiController, AssessmentSubmissionApiController, AssessmentDashboardApiController, RiskAssessmentSectionsApiController, RiskQuestionsApiController, RiskAnswersApiController, MentalCapacityAssessmentApiController, ClinicalScoringController, DnacprOrderApiController, MedicationsApiController, ObservationsApiController, NotesController, PhotosController, PatientsApiController, AiMessageController, WebPubSubController, VersionController
- **Entities:** 14+ — AssessmentEntity, News2ScoreEntity, WaterlowScoreEntity, Phq9ScoreEntity, MentalCapacityAssessmentEntity, DnacprOrderEntity, MedicationEntity, QuestionTemplateEntity, RiskSectionTemplateEntity, RiskQuestionTemplateEntity, MedicalRiskAuditEntity, EmergencyContactEntity, ConsentTypeLabelEntity, AssessmentAnswerEntity
- **Repositories:** 14+ — AssessmentRepository, AssessmentAnswerRepository, WaterlowScoreRepository, MentalCapacityAssessmentRepository, DnacprAcknowledgementRepository, ResponseRepository, SectionRepository, SectionTemplateRepository, SubsectionTemplateRepository, QuestionTemplateRepository, MedicationRepository, PhotoRepository, CareNeedRepository, ConsentTypeRepository
- **Migrations:** 8 Flyway migrations (V1: create tables, V5: add note columns)
- **Key capabilities:**
 - NEWS2 (National Early Warning Score 2) — deterioration detection
 - Waterlow score — pressure injury risk
 - PHQ-9 — depression screening (IAPT-compatible)
 - MentalCapacityAssessmentApiController + MentalCapacityAssessmentEntity — Mental Capacity Act 2005 compliance
 - DnacprOrderApiController + DnacprOrderEntity + DnacprAcknowledgementRepository — resuscitation decision management with acknowledgement audit
 - ClinicalScoringController — automated score calculation for standardised tools
 - AiMessageController — AI-assisted assessment transcription (Azure OpenAI)
 - WebPubSubController — real-time collaborative assessment (multi-assessor support)
 - MedicalRiskAuditEntity — audit trail for risk assessment changes
 - PhotosController — photo evidence capture for wound/pressure injury documentation

Frontend

- **Pages:** Assessment list, assessment detail, section-by-section questionnaire, risk assessment views, MCA assessment, clinical scoring summaries
- **Feature directory:** `src/features/backoffice/clients/` (assessment workflows are accessed via client record)

- **Status:** Real — clients feature has full component structure including assessment workflows

BFF Integration

- **web-bff:** BffAssessmentController, AssessmentWebDashBoardController — GET /assessments/{id}, POST /assessments, GET /assessments/dashboard
- **mobile-bff:** AssessmentsController, RiskAssessmentsController (assessment-client generated OpenAPI client) — GET /assessments/{id}, POST /assessments/submit
- **Generated client:** assessment-client confirmed as generated OpenAPI client in both BFFs

Event Bus

- **Publishes:** `assessment.completed` — DOCUMENTED as trigger for care plan AI generation but NO event publisher class found in assessment-service source
- **Subscribes:** Nothing documented
- **Status:** NOT WIRED — assessment.completed is the first event in the primary clinical workflow chain (Assessment → CarePlan → Schedule → Visit → Finance). Its absence breaks the entire automated care pathway.

Gaps

- No event publisher — assessment.completed cannot trigger automated care plan generation
 - 8 Flyway migrations for 23 controllers is critically low — high probability that schema changes have been applied outside of Flyway migrations, breaking the schema change audit trail required for clinical system governance
 - DNACPR dual-domain: DnacprOrderEntity lives here (correct domain) but DnacprAuditLogEntity lives in identity-service with no confirmed sync mechanism
 - No DoLS (Deprivation of Liberty Safeguards) entity confirmed — DoLS authorisation tracking is a legal requirement for any service user subject to a standard or urgent DoLS authorisation
 - GAD-7 (anxiety screening) not confirmed as a named entity despite PHQ-9 being present — may be handled via generic question templates
-

7. Incidents

Purpose

Manages incident reporting, safeguarding concerns, hazard logging, complaints management, and CQC statutory reporting evidence. Provides CSV export for regulatory data extraction during CQC inspections.

Backend Service

- **Status:** PRODUCTION-READY
- **Controllers:** 7 — AccidentIncidentController, SafeguardingController, HazardController, ComplaintController, LogActionController, SummaryController, CsvExportController
- **Entities:** 9 — AccidentIncidentLog, SafeguardingLog, HazardLog, ComplaintLog, LogAction, LogStatus, LogStatusConverter, SeverityLevel, SeverityLevelConverter
- **Repositories:** 5 — AccidentIncidentLogRepository, SafeguardingLogRepository, HazardLogRepository, ComplaintLogRepository, LogActionRepository
- **Migrations:** 9 Flyway migrations (V4: hazard logs, V7: outbox tables for event publishing)
- **Key capabilities:**
 - SafeguardingLog with reportedToLocalAuthority, localAuthorityReference, reportedToPolice, policeReference — statutory reporting data model at entity level
 - SeverityLevel entity with converter — structured severity classification
 - CsvExportController — regulatory data extraction for CQC inspection evidence
 - SummaryController — aggregate incident reporting across categories
 - V7 outbox migration — reliable event publishing via transactional outbox pattern
 - LogAction + LogActionRepository — action tracking against each incident

Frontend

- **Pages:** `/incidents` (list with filters), incident detail, safeguarding view, incident creation forms
- **Feature directory:** `src/features/backOffice/incidents/` with subdirectories: components, detail, hooks, list, safeguarding, services
- **Status:** Real — full component structure with dedicated safeguarding subdirectory

BFF Integration

- **web-bff:** IncidentsController — GET `/incidents`, POST `/incidents`, GET `/incidents/{id}`, GET `/safeguarding/{id}`
- **mobile-bff:** No incidents controller confirmed — mobile carers cannot report incidents through the BFF layer (PHI boundary gap)

Event Bus

- **Publishes:** `incident.created` (EventPublisher confirmed in source; outbox tables confirmed in V7 migration)
- **Subscribes:** Nothing documented

- **Status:** PARTIALLY WIRED — publisher infrastructure confirmed (outbox tables + EventPublisher class). Notification-service should consume incident.created for safeguarding alerts, but @ServiceBusListener is commented out in notification-service (see Notifications component)

Gaps

- No mandatory reporting deadline field — CQC requires notification within 24 hours for certain incident types (death of service user, serious injuries, allegations of abuse). No notificationDeadline or overdueNotification field confirmed. No automated deadline enforcement or escalation for overdue statutory notifications
 - SafeguardingController endpoint mapping not confirmed — routes may be implemented or stubbed; direct inspection required
 - No MASH (Multi-Agency Safeguarding Hub) integration endpoint or referral number tracking beyond localAuthorityReference
 - Mobile BFF missing incidents reporting controller — field carers cannot submit incident reports through the secured BFF layer
 - No CQC RI (Responsible Individual) notification workflow entity — RI must be notified for certain CQC Regulation 18 events; this is not automated
 - No confirmed near-miss capture category (distinct from accidents) — near-miss data is required for CQC Well-Led evidence
-

8. Finance

Purpose

Manages the complete financial lifecycle: invoice generation, pay rates, payroll, timesheet management, insurance claim generation (837P/837I EDI), remittance reconciliation (835 EDI), gross profit analysis, hours variance reporting, and payer management. The largest service by code volume in the fleet.

Backend Service

- **Status:** PRODUCTION-READY
- **Controllers:** 11 — PayRatesController, PayrollsController, DashboardController, GrossProfitController, InvoiceGroupsController, InvoiceRatesController, PaymentGroupsController, InvoicesController, HoursVarianceController, InsuranceClaimsController, PayerManagementController
- **Entities:** 14 — Invoice, InvoiceGroup, ServiceUserInvoiceGroup, InvoicePayment, Timesheet, TimesheetLineItem, TimesheetBatchJob, PaymentGroup, FinanceDashboardMetric, FinanceAuditLog, OutboxEvent, InsuranceClaim, ClaimLineItem,

RemittanceRecord

- **Repositories:** 10+ — InvoiceGroupRepository, InvoiceLineItemRepository, ServiceUserInvoiceGroupRepository, InvoicePaymentRepository, PaymentGroupRepository, PayRateRepository, InvoiceBatchJobRepository, TimesheetsRepository, FinanceSequenceRepository, OutboxEventRepository
- **Migrations:** 17 Flyway migrations (V1: create tables, V12: unique index on invoice rates)
- **Key capabilities:**
 - 837P/837I EDI billing pathway: InsuranceClaim, ClaimLineItem entities, InsuranceClaimsController, PayerManagementController
 - 835 remittance processing: RemittanceRecord entity, Edi835ProcessorService, RemittanceProcessResponse DTO — full claim-to-remittance cycle
 - Transactional outbox pattern: OutboxEvent entity + OutboxEventRepository — the infrastructure exists for reliable event publishing, but the publisher dispatching to Service Bus is absent
 - TimesheetBatchJob — async batch processing for payroll
 - HoursVarianceController + GrossProfitController — operational finance analytics
 - FinanceDashboardMetric entity — aggregated finance KPIs

Frontend

- **Pages:** `/finance` (billing, payroll views), invoice list/detail, timesheet views, pay rates configuration
- **Feature directory:** `src/features/backOffice/finance/` (api, billing, components, definitions, hooks, models, pages, services, store, types, utils), `src/features/backOffice/billing/`
- **Status:** Real — full component structure confirmed

BFF Integration

- **web-bff:** FinanceBffController (FinanceClientConfig — WebClient, not generated OpenAPI client) — GET /invoices, GET /timesheets, GET /finance/dashboard, GET /gross-profit
- **mobile-bff:** No finance controller — appropriate for field worker role (carers do not access finance)
- **Family portal:** FamilyPortalController includes invoices endpoint (read-only GET confirmed)

Event Bus

- **Publishes:** `invoice.created`, `invoice.paid`, `timesheet.created` — DOCUMENTED but OutboxEvent entity exists without a publisher class dispatching to Service Bus. The outbox pattern is initiated but incomplete.
- **Subscribes:** `visit.completed` — DOCUMENTED as trigger for invoice line item generation but no consumer listener confirmed in finance-service source

- **Status:** NOT WIRED — the transactional outbox infrastructure is started (entity + repository) but the publisher component dispatching messages to Azure Service Bus is absent. Finance events will not fire. The visit.completed subscription is also absent — invoicing cannot be triggered automatically.

Gaps

- OutboxEvent + OutboxEventRepository present but no OutboxEventPublisher class — the transactional outbox is half-implemented; payroll discrepancies and invoice creation events will be silent
 - No confirmed listener for visit.completed — visit-to-invoice automation is broken
 - Non-standard package namespace: com.lumiscare.icon.finance (inconsistent with com.lumiscare.* fleet pattern) — suggests this service was imported or adapted from a separate codebase; introduces dependency drift risk
 - NHS framework invoicing (NHSmail purchase order workflow, ICB/CCG rate card configuration) not confirmed — if this platform targets the UK NHS market, this is a billing gap
 - No ANSI X12 generator class confirmed for outbound 837 claim generation (only inbound 835 processor confirmed)
-

9. Notifications

Purpose

Multi-channel notification dispatch: push (Firebase Cloud Messaging), email (SendGrid), SMS (Twilio), and in-app inbox. Consumes domain events from Azure Service Bus and routes them to appropriate users based on notification preferences and rate limits. Maintains notification history and delivery analytics.

Backend Service

- **Status:** PARTIAL — CRITICAL GAP
- **Controllers:** 5 — DeviceController, InboxController, NotificationPreferencesController, NotificationAnalyticsController, SosNotificationController
- **Entities:** 6 — DeviceRegistration, InAppNotification, NotificationPreference, NotificationTemplate, NotificationLog, NotificationBatchQueue
- **Repositories:** 6 — DeviceRegistrationRepository, InAppNotificationRepository, NotificationPreferenceRepository, NotificationTemplateRepository, NotificationLogRepository, NotificationBatchQueueRepository
- **Migrations:** 4 Flyway migrations (V1: initial schema, V4: notification batch queue)
- **Key capabilities:**

- ServiceBusConfig — Azure Service Bus connectivity configured
- ServiceBusEventListener — exists with handleDomainEvent method
- NotificationEventPublisher — outbound notification.sent/failed events
- NotificationBatchQueue — batch notification infrastructure
- SosNotificationController — direct-call SOS path (bypasses event bus; works independently)
- NotificationPreferencesController — per-user channel preference management
- DeviceController — FCM device token registration
- NotificationAnalyticsController — delivery tracking and metrics

Frontend

- **Pages:** Notification inbox, notification preferences
- **Feature directory:** `src/features/notifications/` (api, components, hooks, pages, services, store, types)
- **Status:** Real — full component structure confirmed

BFF Integration

- **web-bff:** NotificationsController — GET /notifications, PUT /notifications/{id}/acknowledge
- **mobile-bff:** No dedicated notifications controller confirmed — mobile notification delivery is via push (FCM) direct

Event Bus

- **Publishes:** `notification.sent`, `notification.failed` (NotificationEventPublisher confirmed)
- **Subscribes:** visit-events (checkin.timeout, task.flagged), schedule-events (schedule.published), finance-events (invoice.created, invoice.overdue), incidents-events (incident.created) — ALL DOCUMENTED. ServiceBusEventListener EXISTS but @ServiceBusListener annotation is COMMENTED OUT on line 86 of ServiceBusEventListener.java.
- **Status:** CRITICAL — service infrastructure is complete and service can send notifications via direct call. However, @ServiceBusListener is commented out. No domain events from any service are currently being consumed. Missed visit alerts, medication overdue alerts, safeguarding escalations, certification expiry, and schedule change notifications will not be delivered through the event bus pathway.

Gaps

- @ServiceBusListener commented out on ServiceBusEventListener.java line 86 — this is the single most impactful production gap in the entire platform. Uncommenting this line and validating end-to-end event delivery is the highest priority remediation action.

- Only 4 Flyway migrations for a service of this notification scope — migration history appears compressed
 - No dead-letter queue handling or poison message retry strategy confirmed beyond the documented design
 - No confirmed telephony (SMS Twilio) integration test
 - No confirmed deduplication Redis key implementation (documented in design but not confirmed in source)
-

10. Safety

Purpose

Manages lone worker protection (LWP), SOS emergency alerts, and emergency contact management. The LWP timer service runs server-side (not dependent on carer device signal) and escalates overdue check-in sessions through a supervisor notification ladder. This service addresses the CQC requirement for lone worker safety in domiciliary care.

Backend Service

- **Status:** PRODUCTION-READY (Undocumented — no HLD entry exists)
- **Controllers:** 3 — SOSController, LWPController, EmergencyContactController
- **Entities:** 10 — LWPSession, LWPConfiguration, LWPCheckin, LWPEscalation, LWPSessionStatus, SOSEvent, SOSEventType, SOSNotification, EmergencyContact, ResolutionType
- **Repositories:** 7 — LWPSessionRepository, LWPConfigurationRepository, LWPCheckinRepository, LWPEscalationRepository, SOSEventRepository, SOSNotificationRepository, EmergencyContactRepository
- **Migrations:** 2 Flyway migrations (V10: safety tables, V11: add service_user_id to LWP sessions)
- **Key capabilities:**
 - LWPTimerService — scheduled every 30 seconds, finds overdue LWP sessions, triggers escalation ladder (Level 1 to supervisor). Server-side execution — not dependent on carer device or mobile signal
 - LWPEscalation entity + LWPEscalationRepository — persistent escalation audit trail
 - SafetyEventPublisher — publishes LWP escalation events to Service Bus
 - SOSController — emergency SOS event creation and notification dispatch
 - EmergencyContact entity — direct outreach contact management

Frontend

- **Pages:** SOS alert banner on supervisor dashboard (`SOSAlertBanner.tsx`), SOS history page (`SOSHISTORYPage.tsx`), active visits map with SOS overlay (`ActiveVisitsMap.tsx`)
- **Feature directory:** `src/features/backOffice/dashboard/` (SOS components are embedded in supervisor dashboard, not a dedicated safety nav item)
- **Status:** Partial — no dedicated safety nav item; SOS features are integrated into dashboard and notification areas

BFF Integration

- **web-bff:** No dedicated safety BFF controller confirmed — SOS alerts reach care managers via notification-service (`SosNotificationController` direct-call path)
- **mobile-bff:** No safety controller confirmed — mobile SOS trigger path through mobile BFF not confirmed (if mobile calls safety-service directly, BFF auth boundary is bypassed)

Event Bus

- **Publishes:** LWP escalation events (`SafetyEventPublisher` confirmed in source)
- **Subscribes:** Nothing documented
- **Status:** PARTIALLY WIRED — `SafetyEventPublisher` exists. `SosNotificationController` provides a direct-call path to notification-service for SOS alerts (this path works independently of Service Bus)

Gaps

- No dedicated safety navigation item in backOffice sidebar — lone worker protection and SOS are CQC-required features that should be discoverable by care managers and RI without searching the dashboard
- Level 2+ escalation (manager, Responsible Individual, emergency services) not confirmed — only Level 1 (supervisor) notification is confirmed in `LWPTimerService`
- No telephony fallback (IVR) for SOS trigger — mobile app dependency for SOS initiation is a risk if device is compromised, out of power, or carer is incapacitated
- Only 2 Flyway migrations for 10 entity types — schema was created in a single migration; schema change history is compressed
- Mobile BFF does not have a safety controller — mobile SOS trigger path is not secured through the BFF auth layer
- This service has no HLD document, no ADR, and no documented security posture — see ADR-009 stub created alongside this document

11. Policy (AI / RAG)

Purpose

Provides RAG (Retrieval-Augmented Generation) based policy question-and-answer capability. Care workers and managers can ask questions about organisational policies, CQC standards, and care protocols in natural language. The service chunks policy documents, stores vector embeddings, and queries them via Azure OpenAI.

Backend Service

- **Status:** PRODUCTION-READY (Undocumented — no HLD entry, no ADR)
- **Controllers:** 1 confirmed — PolicyRagController (text chunking, vector query)
- **Entities:** Policy document chunks, vector embeddings (exact entity names not confirmed in source grep — implementation uses Azure Cognitive Search or embedded vector store)
- **Repositories:** Not confirmed via static analysis
- **Migrations:** Not confirmed
- **Key capabilities:**
 - PolicyRagController — handles natural language policy queries
 - Text chunking pipeline — policy document preprocessing for vector storage
 - Vector query — semantic search against policy document embeddings
 - Azure OpenAI integration for response generation

Frontend

- **Pages:** AI feature directory exists (`src/features/backOffice/ai/AICarePlanGeneratorPage.tsx`) but no dedicated policy search page confirmed
- **Status:** Stub — ai feature directory contains care plan AI page only; policy search is not wired to a frontend page

BFF Integration

- **web-bff:** No BFF controller for policy RAG confirmed
- **mobile-bff:** No BFF controller for policy RAG confirmed

Event Bus

- **Publishes:** Nothing
- **Subscribes:** Nothing
- **Status:** NOT WIRED — policy-service is not in the Service Bus design

Gaps

- No HLD document, no ADR, no API contract documented
 - No frontend page for policy search — the service is implemented but inaccessible to users
 - No navigation item in backOffice sidebar
 - No documented security posture — policy documents may contain sensitive operational information; access control for policy queries is not confirmed
 - No BFF controller — if accessed directly, PHI boundary enforcement and rate limiting are bypassed
 - See ADR-010 stub created alongside this document
-

12. Document

Purpose

Manages document storage, retrieval, and retention for clinical and operational documents. Uses Azure Blob Storage as the backing store with application-level retention policy enforcement. Supports document upload, categorisation, and time-limited access via pre-signed URLs.

Backend Service

- **Status:** PRODUCTION-READY (Undocumented — no HLD entry, no ADR)
- **Controllers:** 1 confirmed — DocumentController
- **Entities:** Document metadata entity (exact entity name not confirmed)
- **Repositories:** Document metadata repository (not confirmed via static analysis)
- **Migrations:** Not confirmed
- **Key capabilities:**
 - DocumentController — document upload, download (pre-signed URL), list, delete
 - Azure Blob Storage configuration — container management per document category
 - Retention logic — configurable retention periods per document type
 - Document categorisation — clinical vs. operational vs. HR documents

Frontend

- **Pages:** No frontend feature directory confirmed for document management
- **Status:** Not wired — no frontend feature, no navigation item

BFF Integration

- **web-bff:** No document BFF controller confirmed
- **mobile-bff:** BlobStorageController confirmed — handles file upload from mobile (likely used for assessment photos and CV upload, not full document management)

Event Bus

- **Publishes:** Nothing
- **Subscribes:** Nothing
- **Status:** NOT WIRED

Gaps

- No HLD document, no ADR, no API contract
 - No frontend feature or navigation item — document management is inaccessible to care managers despite being implemented
 - No confirmed integration with incidents-service for safeguarding document attachment
 - No confirmed integration with hr-service for staff document management (separate SupportingDocumentController exists in hr-service — potential overlap)
 - Retention logic exists but retention schedule per document category under UK GDPR and NHS Records Management Code of Practice is not documented
 - Mobile BlobStorageController handles photo/file upload but may not route through DocumentController — document provenance tracking is unclear
 - See ADR-011 stub created alongside this document
-

13. FHIR Adapter

Purpose

Exposes FHIR R4 resources (Patient, Observation, MedicationStatement) for interoperability with NHS systems, third-party care management platforms, and referral networks. Enables LumisCare to participate in NHS DSCR (Digitising Social Care Record) programme and GP Connect workflows.

Backend Service

- **Status:** PRODUCTION-READY (Undocumented — no HLD entry, no ADR)
- **Controllers:** 3+ — Patient FHIR provider, Observation FHIR provider, MedicationStatement FHIR provider (confirmed as FHIR R4 providers, not standard Spring controllers)
- **Entities:** FHIR resource mapping layer (not standard JPA entities — FHIR resources are mapped from LumisCare domain model)
- **Repositories:** Delegates to identity-service (Patient), assessment-service (Observation), visits-service (MedicationStatement)
- **Migrations:** None (FHIR adapter is a translation layer, no owned database)
- **Key capabilities:**

- FHIR R4 Patient resource — maps from ServiceUserEntity in identity-service
- FHIR R4 Observation resource — maps from assessment scores (NEWS2, Waterlow, PHQ-9) in assessment-service
- FHIR R4 MedicationStatement resource — maps from MedicationAdministration in visits-service
- NHS DSCR admin nav item exists (`src/features/admin/dscr/`) — this is the only frontend reference to FHIR

Frontend

- **Pages:** `/admin/dscr` (NHS DSCR configuration)
- **Feature directory:** `src/features/admin/dscr/` confirmed
- **Status:** Partial — admin DSCR page exists; no FHIR resource viewer or API explorer for clinical staff

BFF Integration

- **web-bff:** No FHIR BFF controller confirmed
- **mobile-bff:** No FHIR BFF controller confirmed

Event Bus

- **Publishes:** Nothing
- **Subscribes:** Nothing
- **Status:** NOT WIRED

Gaps

- No HLD document, no ADR, no API contract — this is the highest security risk of the four undocumented services. FHIR R4 Patient and Observation resources expose PHI. If fhir-adapter-service is reachable without documented security controls, this is a GDPR and NHS DSPT data protection liability.
 - No documented authentication model for FHIR endpoints — SMART on FHIR app authorisation (required for NHS GP Connect) is not confirmed
 - No BFF controller — FHIR endpoints may be directly exposed without the aggregation, rate limiting, and PHI boundary logging that the BFF layer provides
 - No confirmed CIS2 (NHS Care Identity Service 2) authentication integration — required for NHS-facing FHIR endpoints
 - NHS DSCR admin page exists but is not connected to a live FHIR endpoint through a BFF
 - See ADR-012 stub created alongside this document
-

14. Web BFF

Purpose

Backend-for-Frontend aggregation layer for the React 19 web application. Orchestrates parallel and sequential calls to microservices, aggregates responses, enforces JWT validation, applies rate limiting (via Azure API Management), and provides OpenAPI-generated typed client contracts. Port 8080.

Backend Service

- **Status:** PRODUCTION-READY
- **Controllers:** 22 — DashboardController, SupervisorDashboardController, SchedulingController, VisitsController, CarePlanController, ServiceUsersController, UsersController, EmployeeController, IncidentsController, BffAssessmentController, AssessmentWebDashBoardController, FamilyPortalController, HrComplianceController, FinanceBffController, CalendarController, CompletedEventsController, HandoffController, ReportsController, OrganizationsController, NotificationsController, ResumeUploadController, CqcReadinessController
- **Generated OpenAPI clients:** 4 of 10 services — assessment-client, careplan-client, hr-client, incidents-client
- **WebClient-based (not generated):** visits-service (VisitsController), scheduling-service (SchedulingController + CalendarController), finance-service (FinanceBffController + FinanceClientConfig), notification-service (NotificationsController + FamilyPortalController)
- **Unintegrated services:** safety-service (no dedicated BFF controller), policy-service (no controller), document-service (no controller), fhir-adapter-service (no controller)
- **Key capabilities:**
 - FamilyPortalController confirmed read-only (GET patterns only, no POST/PUT/PATCH) — PHI minimum-necessary for family access
 - CqcReadinessController — dedicated endpoint for CQC inspection evidence aggregation (clinically significant governance feature)
 - DashboardController + SupervisorDashboardController — parallel microservice call aggregation for management views
 - HrComplianceController — DBS, training certificate, and compliance expiry aggregation

Frontend Integration

- **Target:** All `src/features/backOffice/` components, `src/features/familyPortal/`, `src/features/admin/`
- **Current state (gap):** Frontend CLAUDE.md reveals the web app currently calls the old Django monolith (`app-lumiscare-dev-uks-001.azurewebsites.net`) through manual axios

wrappers. `src/api/generated/` directory is scaffolded but contains no generated client files. `yarn generate:api` is documented but not operational.

BFF Integration

- **web-bff:** IS the BFF — self
- **mobile-bff:** N/A

Event Bus

- **Publishes:** Nothing (BFF is stateless aggregation layer)
- **Subscribes:** Nothing
- **Status:** N/A

Gaps

- 6 of 10 microservices use WebClient with manual configuration rather than generated OpenAPI clients — contract drift risk as service APIs evolve
 - safety-service, policy-service, document-service, and fhir-adapter-service have no BFF controller — these services are either inaccessible from the web frontend or are called directly (bypassing auth boundary)
 - Frontend is currently routing to old Django monolith, not to web-bff — the BFF is built but not yet the live API target for the web app
 - OpenAPI client generation pipeline (`yarn generate:api`) is not operational — manual axios wrappers create inevitable contract drift at scale
 - No confirmed Redis caching layer in BFF for high-frequency identity lookups (documented as 24h TTL in Integration Matrix)
-

15. Mobile BFF

Purpose

Backend-for-Frontend aggregation layer for the React Native / Expo field worker mobile application. Provides a minimal, mobile-optimised API surface for care execution: care plan read access, appointment viewing, assessment submission, risk assessment, and blob storage for photos. Port not confirmed.

Backend Service

- **Status:** PARTIAL — HIGH RISK
- **Controllers:** 6 — CarePlanController, AppointmentsController, CarerScheduleController, AssessmentsController, RiskAssessmentsController, BlobStorageController
- **Generated OpenAPI clients:** 2 of 10 services — assessment-client, careplan-client
- **WebClient-based:** MobileVisitsClient (visits-service via CarerScheduleController and AppointmentsController)
- **Key capabilities:**
 - AppointmentsController — GET /my-appointments, appointment detail
 - CarerScheduleController — GET /my-visits/today, visit schedule
 - AssessmentsController + RiskAssessmentsController — assessment submission for field assessments
 - BlobStorageController — photo and document upload from mobile (assessment photos, CV upload)
 - CarePlanController — read-only care plan access for visit execution context

Frontend Integration

- **Target:** `mobile/app/` (React Native / Expo SDK 52)
- **Coverage:** Care plan, assessments, appointments, visit schedule

BFF Integration

- **web-bff:** N/A
- **mobile-bff:** IS the BFF — self

Event Bus

- **Publishes:** Nothing
- **Subscribes:** Nothing
- **Status:** N/A

Gaps

- No eMAR controller — mobile carers cannot record medication administration through the BFF (HIPAA minimum-necessary enforcement gap if calling visits-service directly)
- No EVV dedicated controller — check-in/check-out is routed via CarerScheduleController/MobileVisitsClient but not through a dedicated EVV compliance controller with explicit 6-data-element capture
- No incidents controller — mobile carers cannot report incidents through the BFF
- No SOS / safety controller — mobile SOS trigger path is not secured through the BFF auth layer
- No vital signs controller — carer observation and vital sign recording during visits bypasses BFF

- No care note controller — care note recording during visits bypasses BFF
- Only 2 generated OpenAPI clients (assessment-client, careplan-client) — 8 services accessed without typed contracts
- No offline sync protocol confirmed at BFF layer — offline-first capability documented as a mobile feature but sync conflict resolution through BFF is not specified

Event Bus Summary Table

Event	Producer	Publisher Code?	Consumer	Listener Code?	Status
assessment.completed	assessment-service	NO	careplan-service	NO	NOT WIRED
careplan.published	careplan-service	NO	scheduling-service	CarePlanEventIdempotencyEntity (ready)	NOT WIRED
careplan.updated	careplan-service	NO	visits-service	NO	NOT WIRED
schedule.published	scheduling-service	AppointmentEventPublisher YES	notification-service	@ServiceBusListener COMMENTED OUT	BROKEN
schedule.updated	scheduling-service	AppointmentEventPublisher YES	visits-service	NO	PARTIALLY WIRED
visit.checkedin	visits-service	VisitEventPublisher YES	notification-service	@ServiceBusListener COMMENTED OUT	BROKEN
visit.completed	visits-service	VisitEventPublisher YES	finance-service	NO	PARTIALLY WIRED
task.flagged	visits-service	VisitEventPublisher YES	notification-service	@ServiceBusListener COMMENTED OUT	BROKEN
checkin.timeout	visits-service	VisitEventPublisher YES	notification-service	@ServiceBusListener COMMENTED OUT	BROKEN
assistance.requested	visits-service	VisitEventPublisher YES	notification-service	@ServiceBusListener COMMENTED OUT	BROKEN
invoice.created	finance-service	OutboxEvent entity only — NO publisher	notification-service	@ServiceBusListener COMMENTED OUT	NOT WIRED
invoice.paid	finance-service	NO	notification-service	@ServiceBusListener COMMENTED OUT	NOT WIRED

Event	Producer	Publisher Code?	Consumer	Listener Code?	Status
timesheet.created	finance-service	NO	notification-service	@ServiceBusListener COMMENTED OUT	NOT WIRED
employee.created	hr-service	HrEventPublisher YES	identity-service	NO confirmed listener	PARTIALLY WIRED
employee.terminated	hr-service	HrEventPublisher YES	scheduling-service	NO	PARTIALLY WIRED
availability.updated	hr-service	HrEventPublisher YES	scheduling-service	AvailabilityUpdatedEventListener YES	WIRED
leave.approved	hr-service	HrEventPublisher YES	scheduling-service	NO confirmed listener	PARTIALLY WIRED
incident.created	incidents-service	EventPublisher YES (outbox)	notification-service	@ServiceBusListener COMMENTED OUT	BROKEN
notification.sent	notification-service	NotificationEventPublisher YES	analytics-service	NOT IMPLEMENTED	PARTIALLY WIRED

Summary: HR → Scheduling (availability.updated) is the only fully wired event chain. The primary clinical workflow (Assessment → CarePlan → Scheduling → Visits → Finance) has broken links at every node.

Priority Remediation Register

P0 — Patient Safety and Compliance Blocking

P0-001: Uncomment @ServiceBusListener in notification-service

- File: `backend/services/notification-service/src/main/java/.../ServiceBusEventListener.java` line 86
- Impact: All event-driven alert delivery (missed visit, medication overdue, LWP escalation, safeguarding) is non-functional
- Effort: Minimal code change; requires end-to-end event delivery validation for all subscribed event types

P0-002: Resolve DNACPR dual-domain ownership

- DnacprOrderEntity in assessment-service + DnacprAuditLogEntity in identity-service with no sync mechanism
- Impact: Resuscitation decision ambiguity is clinically unacceptable

- Resolution: Either consolidate into assessment-service (correct domain) with identity-service holding a reference, or implement a confirmed event-driven sync pattern

P1 — Regulatory Exposure

P1-001: Add event publisher to assessment-service for assessment.completed

- Breaks the Assessment → CarePlan AI generation automated pathway

P1-002: Add event publisher to careplan-service for careplan.published

- Breaks the CarePlan → Scheduling automated pathway

P1-003: Add mobile BFF controllers for eMAR, EVV, incidents, and SOS

- Or document and formally enforce direct-service access security boundary with compensating controls

P1-004: Implement mandatory notification deadline and automated escalation in incidents-service

- CQC Regulation 18 requires notification within 24 hours for certain incident types

P1-005: Document and security-review fhir-adapter-service

- FHIR R4 Patient/Observation endpoints may expose PHI without documented authentication controls
- NHS DSPT and GDPR exposure

P2 — Architecture Integrity

P2-001: Implement OutboxEventPublisher in finance-service

- Completes the transactional outbox pattern already started

P2-002: Add finance-service listener for visit.completed event

- Enables automatic invoice line item generation from visit completion

P2-003: Confirm EmarController enforces witness requirement at service layer

- Entity fields exist; business logic enforcement must be verified

P2-004: Add Flyway migrations to bring visits-service (7) and assessment-service (8) in line with entity complexity

P2-005: Standardise finance-service package namespace from com.lumiscare.icon.finance to com.lumiscare.finance

P2-006: Operationalise yarn generate:api pipeline

- Without generated clients, frontend contract drift is inevitable as microservice APIs evolve

Architectural Risks

Risk	Severity	Description
BFF-less frontend in production	CRITICAL	Frontend routes to old Django monolith, not web-bff. All microservices are bypassed.
Broken clinical workflow event chain	HIGH	Assessment → CarePlan → Schedule → Visit → Finance has multiple broken publisher/subscriber links
Notification service deaf to event bus	HIGH	@ServiceBusListener commented out — all event-driven alerts are non-functional
Four undocumented services in production path	HIGH	safety, policy, document, fhir-adapter — no API contracts, no security posture
FHIR PHI exposure	HIGH	FHIR R4 resources expose PHI without documented authentication controls
Finance event bus gap	MEDIUM	Transactional outbox started but publisher absent — billing events are silent
Mobile BFF coverage gap	HIGH	eMAR, EVV, incidents, SOS absent from mobile BFF — direct service calls bypass auth boundary
DNACPR dual ownership	HIGH	Resuscitation decision data in two services with no confirmed sync
CQC mandatory notification deadline	MEDIUM	No automated enforcement for 24-hour statutory reporting requirement
OpenAPI client drift	MEDIUM	6 of 10 services accessed via manual WebClient — contract drift inevitable

Document History

Version	Date	Author	Changes
---------	------	--------	---------

1.0	2026-04-04	Dr. Sarah Chen	Initial — 13 components + 2 BFFs documented. Evidence base: static filesystem analysis + HLD document review. Cross-reference with lumiscare-backend-llid.md and lumiscare-hld-gap.md.
-----	------------	----------------	---

Revision #2

Created 2026-04-05 21:40:48 UTC by John

Updated 2026-05-31 20:05:32 UTC by John