LumisCare

LumisCare client project (beta)

Overview

Overview

Domain & Infrastructure

- **Domain:** `TBD`
- **Vercel Project:** `N/A`
- **Local Repository:** `~/projects/client/lumiscare-beta`
- **Remote Repository:** `Unknown`
- **Tech Stack:** Java Spring Boot, Mobile BFF, Web BFF

Deploy Method

Unknown — requires discovery

Quick Links

- Live Site: TBD

Architecture

Architecture

Technology Stack

Java Spring Boot, Mobile BFF, Web BFF

Infrastructure

To be documented: hosting environment, dependencies, integrations

Deployment Pipeline

Unknown — requires discovery

Dependencies

To be documented: external services, APIs, databases

Deploy Runbook

Deploy Runbook

Prerequisites

- Access to repository: `~/projects/client/lumiscare-beta`
- Vercel CLI installed: `npm i -g vercel`
- Authenticated: `vercel login`

Deployment Steps

1. **Navigate to repo:** `cd ~/projects/client/lumiscare-beta`
2. **Pull latest:** `git pull origin main`
3. **Deploy:** `Unknown — requires discovery`
4. **Verify:** Check TBD

Rollback Procedure

1. **List deployments:** `vercel ls N/A`
2. **Identify previous stable deployment ID**
3. **Rollback:** `vercel rollback [deployment-url]`

Common Issues

To be documented as issues are discovered

Current State

Current State

What Works

- *To be documented*

What Doesn't Work / Known Issues

- *To be documented*

Open Tasks

Link to Mission Control tasks related to this project

Last Verified

Date: 2026-04-15

Status: Initial documentation shell created

Changelog

Changelog

2026-04-15 — Documentation Shell Created

- Initial BookStack book structure created
- Overview, Architecture, Deploy Runbook, Current State pages added
- Task: `#7763` (DOD System: BookStack Shell per projekat)

All significant deploys and changes should be logged here with date, description, and deploy ID.

LumisCare Privacy Terms Readiness Options — 2026-05-24

LumisCare Privacy/Terms readiness options

Date: 2026-05-24 Status: implementation drafted after CEO direction on 2026-05-24; final legal review still recommended before treating as full SaaS legal package.

Current live gap

`landing/index.html` footer currently renders:

- `Privacy` with `href="#"`
- `Terms` with `href="#"`
- `Contact` with `mailto:hello@lumiscare.com`

Mail contact is verified separately, but Privacy/Terms remain unresolved public-readiness blockers because the public landing page promotes care-management software and repo documentation references regulated healthcare/care contexts.

Existing product/compliance context found in repo

Relevant repo context to review before approving legal pages:

- `docs/FAMILY-PORTAL-INDUSTRY-GUIDE.md` references UK care/CQC/GDPR-oriented family portal expectations.
- `docs/INFRASTRUCTURE-DOCUMENTATION-REVIEW.md` flags US healthcare/HIPAA documentation as a critical gap.

- `docs/design/SAFETY-COMPLIANCE-FEATURES-DESIGN.md` references GDPR/CCPA/HIPAA considerations for safety/compliance features.
- `docs/design/MEDICATION-VITALS-DESIGN.md` references HIPAA Security Rule considerations.

These docs are product/engineering context only; they do not constitute approved public legal policy.

Decisions required before publishing final legal pages

1. **Legal entity/controller**
   - Which company is the contracting/provider entity for LumisCare?
   - Registered address and contact email for privacy requests.
2. **Geography and market scope**
   - UK only, US only, EU/EEA, Norway, or multi-region?
   - Whether public copy should mention CQC/DSCR/HIPAA/GDPR commitments now or only after compliance sign-off.
3. **Data roles**
   - Is LumisCare a processor/vendor for agencies, a controller for demo leads, or both?
   - Are family/care-recipient data flows live today or only planned?
4. **Data collected by the landing page**
   - Current landing CTA uses mailto, not a web form.
   - Confirm whether analytics, cookies, Application Insights, CRM ingestion, or tracking pixels are enabled on public landing.
5. **Healthcare/sensitive data posture**
   - Confirm whether visitors should be warned not to send patient/PHI/sensitive care data via email demo contact.
   - Confirm breach/contact escalation wording.
6. **Terms scope**
   - Public marketing-site Terms only, or SaaS subscription Terms as well?
   - If SaaS Terms: pricing, trial, cancellation, acceptable use, support SLA, liability limits, DPA/BAA references need legal approval.

Safe implementation options

Option A — Minimal blocker acknowledgement, no public legal pages yet

Keep Privacy/Terms as known blockers in readiness docs. Do not claim full public readiness.

Pros:

- No fabricated legal policy.
- Lowest legal risk.

Cons:

- Live footer has dead `href="#"` links.
- Not ideal for public launch/trust.

Option B — Publish “review pending” placeholder pages

Create `/privacy.html` and `/terms.html` that clearly state legal documents are pending review and provide `hello@lumiscare.com` contact.

Pros:

- Removes dead links.
- Honest about status.

Cons:

- Placeholder legal pages may still look unprofessional.
- Does not satisfy full compliance/legal-readiness.

Option C — Publish approved marketing-site Privacy/Terms only

Legal/CEO approves narrow pages covering:

- demo/contact email handling,
- no patient data via email,
- no cookies/analytics or explicit cookie disclosure if present,
- controller/contact details,
- user rights by target geography,
- marketing site usage terms.

Pros:

- Best near-term public landing readiness.
- Avoids premature SaaS/PHI commitments.

Cons:

- Requires legal/entity decisions above.

Option D — Publish full SaaS Privacy, Terms, DPA/BAA package

Full legal suite for production SaaS and regulated healthcare data.

Pros:

- Best long-term enterprise readiness.

Cons:

- Highest legal workload.
- Should not be generated or published without legal review.

CEO direction received 2026-05-24

- Responsible legal/operator entity for LumisCare public site: Snowit.
- Market posture: EU-first and US-aware.
- Option C approved: narrow marketing-site Privacy/Terms first.
- Footer links may be updated to `/privacy.html` and `/terms.html` after pages are added.

Implemented draft

Implemented narrow marketing-site pages:

- `landing/privacy.html`
- `landing/terms.html`

The pages intentionally do not claim to be a full SaaS legal package, DPA, BAA, or customer contract. They cover the public marketing website and demo enquiries, and warn visitors not to send patient/care-recipient/PHI/sensitive care data by email.

Remaining legal hardening recommended later:

1. Confirm exact registered Snowit legal name, registration number, and address for formal insertion.
2. Confirm cookie/analytics status if tracking is added later.
3. Add full SaaS Terms, DPA, and BAA package before regulated production customer onboarding.

Deployment verification summary

LumisCare PR #2 legal pages deploy verification

Date: 2026-05-24 UTC

Merge/deploy

- PR #2: https://github.com/johnatbasicas/vivacare/pull/2
- Merge commit: `ce71a014803d9de18227989c8e57d31155812dce`
- GitHub Actions run: https://github.com/johnatbasicas/vivacare/actions/runs/26372435887
- Workflow conclusion: `success`
- Jobs passed:
  - Deploy: landing (lumiscare.com)
  - Deploy: backoffice (app.lumiscare.com)
  - Deploy: admin (admin.lumiscare.com)
  - Deploy: family-portal (family.lumiscare.com)
  - Smoke Test: verify all portals

Evidence:

- `/tmp/alai/lumiscare-legal-live-verify-20260524T205500Z/gh-run-view-26372435887-final.json`
- `/tmp/alai/lumiscare-live-verify-20260524T195900Z/gh-run-watch-26372435887.txt`

Live browser verification

Verdict: `PASS`

Verified on `https://lumiscare.com`:

- `/` returns HTTP/browser 200.
- `/privacy.html` returns HTTP/browser 200.
- `/terms.html` returns HTTP/browser 200.
- Footer links point to `/privacy.html` and `/terms.html`.
- No remaining `href="#"` links on landing.

- No browser page errors detected.
- Tailwind CDN/config runtime issue remains absent.
- Live page hashes match `origin/full-production` for landing, privacy, and terms pages.
- Screenshots captured for all three pages.

Evidence:

- `/tmp/alai/lumiscare-legal-live-verify-20260524T205500Z/live-legal-browser-verification.json`
- `/tmp/alai/lumiscare-legal-live-verify-20260524T205500Z/live-home.png`
- `/tmp/alai/lumiscare-legal-live-verify-20260524T205500Z/live-privacy.png`
- `/tmp/alai/lumiscare-legal-live-verify-20260524T205500Z/live-terms.png`

Scope note

The published pages are narrow marketing-site Privacy Notice and Website Terms for demo/contact enquiries. They are not a full SaaS legal package, DPA, BAA, or regulated production customer contract set.

Runbook — LumisCare "Unable to load your account" (Entra B2B + JIT/DB mapping) — 2026-06-02

Runbook — LumisCare "Unable to load your account" (Entra B2B + JIT/DB user mapping)

Date: 2026-06-02 · **Evidence:** `/tmp/evidence-session-fe5379ce/` · **Env:** ALAI demo (Azure tenant `3454a03f`, `rg-lumiscare-demo`) · **App:** `app.lumiscare.com`, appId `e422174a-24a6-4889-b66c-f6c483b8631f`

Symptom

After login, the backoffice shows **"Unable to load your account — We could not retrieve your user information."** Rendered by `frontend/packages/shared-ui/src/components/layout/AccountInfoLoader.tsx` when the `GET /users/about-me` query (in `useAccountStore.ts`) errors.

Root cause (NOT a password problem)

A Microsoft **Entra B2B / admin-consent / backend user-mapping** problem. A logged-in guest (`alem@alai.no`, Entra OID `f9275cf4-…`) authenticated, but was **not correctly provisioned/mapped** to a LumisCare DB user + org, so `/users/about-me` could not return a usable account.

What is NOT the cause (verified, do not chase again)

- Backend `GET /api/v1/users/about-me` returns **HTTP 200** with a valid shape for a correct token.
- **CORS** is fine — `CorsConfig` uses `allowedHeaders("*")`, `app.lumiscare.com` allowed, credentials true; `OPTIONS` preflight → 200.
- Frontend **env** is correct — `LUMISCARE_CLIENT_ID` / `LUMISCARE_BACKEND_CUSTOMER_CLIENT_ID` = `e422174a`, scope `api://e422174a/api`.
- **Data exists** — `/service-users` = 15, `/hr/employees` = 10 for org `f714cc2f`.
- Deployed tree = `frontend/packages/backoffice` + `shared-ui` (NOT legacy `frontend/web/`).

Fix (live, in order)

1. **Entra B2B invite** (re)issued for `alem@alai.no` — `lumiscare-b2b-invite.json` / `alem-fresh-invite.txt`.
2. **MSAL config confirmed** correct for `app.lumiscare.com` — `uat-login-diagnosis.md`.
3. **Admin consent grant** repaired for the LumisCare app:
   - scope: `api openid profile offline_access`, `consentType=AllPrincipals`
   - Grant ID: `Tucgg8C0XUKt_DONAFF0Tk7nIIPAtF1CrfwzjQBRdE4`
4. **Backend BFF/JIT + DB user mapping** (the decisive step — frontend deploy/JIT merge alone was NOT enough):
   - `alem@alai.no` promoted directly in Postgres: DB id `eccfeb0c-0b12-4439-9b99-33a12f9110c5`, status `ACTIVE`, org `f714cc2f-a0fc-4e47-9164-baa540fd820f` (Sunshine Home Care LLC), role `system_admin`.
   - JWT linkage: Entra OID `f9275cf4-…` → DB user UUID (via JIT).
   - Backend revs: **identity** `--0000008` (issuer URI + audience GUID match), **web-bff** `--0000032` (audience-permissive + `/users` alias), Hibernate `ddl-auto=update` for schema drift.

Proof

- `bff-about-me-success.txt` → `HTTP=200`, org `f714cc2f`, account `eccfeb0c…`, email mapped from OID.
- `alem-user-record-promoted.txt` → promoted DB record.

Key lesson

For a new Entra guest, **a frontend deploy / JIT merge is not sufficient**. A working login requires the backend chain: **Entra B2B membership + admin consent + identity-service JIT + an ACTIVE DB user mapped to an org**. When "Unable to load account" recurs for a new user → check the **DB user + org mapping** and **admin consent**, not the password or the frontend.

Related security debt

- Demo enablement temporarily relaxed identity-service security; track revert + proper app-roles (MC #102747).

LumisCare CI — Snyk + Lighthouse for deployed packages (MC #102842) — 2026-06-03

Summary

MC #102842 re-adds **Snyk** (dependency scan) and **Lighthouse** (performance) CI jobs to `.github/workflows/ci.yml` for the **deployed** pnpm packages, replacing the placeholder TODOs left by MC #102817 (which removed the old jobs that scanned the dead `frontend/web/` tree).

- **Repo:** github.com/johnatbasicas/vivacare — branch `ci/snyk-lighthouse-packages-102842` → **PR #43** (base `dev`)
- **Fix commit:** `1ed9f107`

What was added

`security` job (Snyk)

- Scans deployed packages: `frontend/packages/{backoffice,admin,family-portal}/package.json`
- Auth via `${{ secrets.SNYK_TOKEN }}` only — **never hardcoded**
- `--severity-threshold=high`
- **Advisory / non-blocking** (`continue-on-error: true`); NOT in the blocking `quality-gate` `needs:`
- **Graceful degrade:** a guard step checks the token; if absent it emits a `::warning::` and skips the scans (job stays success) rather than hard-failing

`lighthouse` job

- Runs `lhci collect` against the **live** SWA URLs — `app.lumiscare.com`, `admin.lumiscare.com`, `family.lumiscare.com`
- Does **not** build the dead `frontend/web/` tree

- Advisory / non-blocking

Defect caught + fixed before close

First CI run (`26888003662`) the Snyk job died at `pnpm install --frozen-lockfile` with `ERR_PNPM_IGNORED_BUILDS` (exit 1) — `pnpm/action-setup@v4 version: latest` resolved to pnpm v10, which treats ignored build scripts as a hard error. `deploy.yml` pins `PNPM_VERSION: "9"` (warn only). **Fix:** pin pnpm 9 + add pnpm cache, mirroring `deploy.yml`.

Verification

- FINAL CI run **26888884509** = `completed/success`; all 5 jobs success (backend-test, security, lighthouse, code-scan, quality-gate REQUIRED).
- Snyk install step success (641 pkgs); guard fired (`skip=true`, token absent); scans skipped; job success.
- Independent verifier subagent: **13/13** atomic claims PASS.
- Company Mesh P2P pre-verifier (eval/Proveo): **PASS** — `mesh-thr-105cdec0-7dd4-4370-adb0-271547da635a`.
- til-done verdict: **DONE** — receipt `/tmp/til-done/102842-20260603T135849Z.json`.

Standing CEO action

Add **`SNYK_TOKEN`** to the `johnatbasicas/vivacare` repo secrets (Settings → Secrets → Actions) to activate real Snyk scanning. Until then the job skips cleanly with a warning. (John's PAT lacks `secrets:write` — HTTP 403.)

LumisCare Wave-1 Durability Redeploy & Validation — 2026-06-11

LumisCare Wave-1 Durability Redeploy & Validation — 2026-06-11

Scope

MC #103376 / parent #103260: prove Wave-1 live artifacts are durable after merge to `dev`, rebuilt and redeployed from merged `dev`, then independently validated.

Source and live artifacts

- Source commit: `b4e0518f88981248a12a1bee071a6b169ea292c5` (`fix: preserve identity Flyway migration checksums`).
- Backend images:
  - `lumiscaredemo.azurecr.io/lumiscare-web-bff:dev-b4e0518f8898`, ready revision `lumiscare-web-bff--0000065`.
  - `lumiscaredemo.azurecr.io/lumiscare-identity:dev-b4e0518f8898`, ready revision `lumiscare-identity--0000025`.
- Static Web App bundles:
  - Backoffice: `assets/index-CBr5dOPC.js`.
  - Admin: `assets/index-DvWxQs6Z.js`.

Validation verdict

Independent Proveo validation: **PASS 8/8**, regressions: `[]`, apiOk: `6`.

Validated live areas:

1. Backoffice smoke / deployed bundle confirmation.
2. Dashboard real data, no mock/hardcoded numbers, no crash.
3. EVV no regression.
4. Scheduling opens for care-manager, no access denied.
5. Admin loads / AD-001 behavior intact.
6. Audit logs page uses honest real/empty data and no fabricated rows.
7. Compliance page has no fake 95% and no fake PHI rows.
8. Family portal smoke/no white screen.

Evidence paths

- Redeploy summary: `/Users/makinja/system/evidence/lumiscare-wave1-durability-b4e0518f8898/wave1-durability-redeploy-summary.md`
- Orchestrator self-check summary: `/Users/makinja/system/evidence/lumiscare-wave1-durability-b4e0518f8898/wave1-selfcheck-summary.md`
- Orchestrator self-check JSON: `/Users/makinja/system/evidence/lumiscare-wave1-durability-b4e0518f8898/wave1-live-revalidation-selfcheck.json`
- Independent Proveo validation JSON: `/tmp/alai/1ed4537f/evidence-wave1-independent/INDEPENDENT-VALIDATION.json`
- Contract validator JSON: `/tmp/evidence-103376/verification.json`
- Ack / next-unit evidence: `/Users/makinja/system/evidence/lumiscare-wave1-pass-ack-next-unit-20260611.md`
- Independent screenshots: `/tmp/alai/1ed4537f/evidence-wave1-independent/screenshots/`

Decision

Wave-1 durability gate is cleared. Wave-2 can proceed when ready, with separate gates for ADO org creation and leaked credential rotation (#103380). Do not activate unsafe pipeline paths that touch old leaked secrets.