CareFWD — Security & Data Overview

For hospital IT, InfoSec and compliance reviewers. Live version: care-fwd.com/security

Version 1.0
September 24, 2026

WHAT CAREFWD IS

A care routing network for hospital discharge planners: the step *before* a referral. A planner posts an anonymous Care Transition Query, matching post-acute providers answer whether they can take the case, and the planner chooses. The referral itself, with the patient's identity, happens in your existing systems. CareFWD is not an EHR, not a PHI-carrying referral system, and not a payer directory.

WHAT WE HOLD, AND WHAT WE DON'T

Data	Held?	Notes
Patient identity (name, DOB, MRN, SSN, address, phone)	**No**	There is no field for it. Identifier-shaped text is blocked at entry and again server-side.
Care Transition Query	**Yes, anonymous**	Care category, destination ZIP, payer type, free-text needs. No patient identity.
Care manager and provider accounts	**Yes**	Name, work email, title, role, organization. Passwords are handled and hashed by the authentication provider, never stored by CareFWD.
Facility and provider business data	**Yes**	Public business information: address, phone, fax, website, NPI, CMS rating.
Clinical records, referral packets, insurance member IDs	**No**	These stay in your hospital's referral workflow and systems.

WHERE IT RUNS

- Application served by Cloudflare's network (TLS termination, DDoS mitigation) in front of every request.
- Database, authentication and file storage on Supabase, AWS region ca-central-1 (Montréal, Canada).
- Encrypted in transit (TLS 1.2+, HSTS enforced) and at rest (AES-256 on the database provider's storage).
- Automated daily database backups by the database provider.
- No data is sold, and none is used for advertising.

WHO CAN SEE WHAT

- Every account is approved by a CareFWD administrator before it can see anything; no one can grant themselves elevated access.
- Role-based access: planners, provider representatives and administrators each see only their own surface.
- Row-level security enforced inside the database on every table, so access rules hold even if application code has a bug.
- Privileged service credentials exist only on the server, never in a browser.
- Administrative actions are written to an audit log; every contact-sharing consent is recorded in an append-only ledger enforced by the database.
- Idle-session timeout is built in and can be enabled per deployment. Multi-factor authentication for user accounts is on the near-term roadmap.

HOW WE OPERATE

- Secrets live in the hosting provider's encrypted secret store, never in source code, with a written rotation runbook.
- Every change passes code review, an automated test suite (type checks, lint, unit, browser and database regression tests) and required status checks before production.
- Dependencies updated on a weekly automated schedule.
- Security headers on every response: Content-Security-Policy allowlist, HSTS, frame denial, referrer and permissions policies.
- Analytics run on public marketing pages only, never inside the logged-in portals.

COMPLIANCE POSTURE, STATED PLAINLY

> CareFWD is architected so that no protected health information is stored or transmitted through the platform. We do not currently hold a SOC 2 report. Our controls are aligned to the SOC 2 Trust Services Criteria and the HIPAA Security Rule safeguards, and a SOC 2 audit is planned as customer volume grows. We will complete your vendor security questionnaire (SIG Lite, HECVAT or your own form) and will sign a Business Associate Agreement if your review determines one is required.

SUBPROCESSORS

Provider	Purpose	Location
Cloudflare	Application hosting, DNS, TLS, DDoS mitigation, inbound email routing	Global edge; US-based company
Supabase	PostgreSQL database, authentication, file storage	AWS ca-central-1 (Montréal, Canada)
Google Analytics 4	Visit counts on public marketing pages only; never inside the portals	United States
Google Maps Platform (Places)	Server-side lookup of facility business details	United States
CMS.gov and NPPES (public datasets)	Provider ratings and NPI validation; outbound reads only	United States

REPORTING A SECURITY CONCERN

Write to **security@care-fwd.com**. We acknowledge reports within two business days. If we confirm an incident affecting your organization's data, we notify you within 72 hours of confirmation with what happened, what was affected and what we are doing about it. For network allow-listing, the domains to permit are **care-fwd.com** and ***.care-fwd.com** (category: Health & Medicine / Business).