Security overview

CarePath247 — audit-ready care operations for Ontario residential, foster, group home and supported living programs. A product of Paqads Consulting Inc., an Ontario, Canada company. Hosted in Canada.

This is a one-page summary for a compliance lead who needs something to forward. Every statement here is published at carepath247.com/security, where each one is set out in full. Nothing on this page is a certification claim; what we have *not* done is listed at the bottom, in the same words.

Where the data lives

Hosting	AWS Canada (Central), Ontario.
Backups	In Canada.
In normal operation	Records, files, backups and credentials do not leave the country.
Availability	PostgreSQL running Multi-AZ with automatic failover, so a single data-centre failure does not take an agency offline.

The controls

One agency cannot see another. Tenant isolation is enforced in three independent layers: a separate portal per agency on its own subdomain; application role-based access, scoped to the individual home rather than the whole agency; and PostgreSQL row-level security, enabled and forced on every table holding personal information. The third layer is the one that matters — isolation does not depend on application code being correct. A query that forgets its tenant context returns zero rows rather than someone else's data, because the database refuses it, not the application.

Encryption. Everything at rest — database, uploaded files, backups and application secrets — is encrypted under a customer-managed KMS key with automatic annual rotation, rather than a shared default key. Key access is scoped to the application roles that need it, and every use is recorded in AWS CloudTrail. TLS 1.2 or better in transit, at the edge and between the application and the database.

The audit trail is append-only, and records reads. Opening a record, downloading a document and running an export are all logged to a named account, not just writes. Audit visibility itself follows the role hierarchy, so the trail cannot be used as a way around the access model.

Records lock on approval. Corrections are signed, dated amendments that sit alongside the original, which never changes. An agency can also switch on a faint watermark naming the person signed in, the agency and the time, on screen and on anything printed — so a photographed or photocopied record traces back to an account.

Two-factor authentication. TOTP is available on any account, and an agency can require it of everyone.

Outbound email carries no client names and no health detail. Alerts and counts only; everything specific sits behind authentication. This is a PHIPA position, not a style preference.

The regulatory frame

CarePath247 is built for organisations operating under **PHIPA**, **CYFSA Part X**, Ontario child/youth services licensing, and **AODA** accessibility obligations. A **Privacy Impact Assessment** and a **Data Processing Agreement** are available on request, along with the technical-measures annex used to answer security questionnaires.

The agency remains the custodian of its records and is responsible for determining its own role and obligations under that legislation. CarePath247 does not, by itself, satisfy an agency's licensing, clinical, ministry or professional obligations; it provides the controls — audit trails, access scoping, retention support — that help an agency meet them.

What we have not done yet

Published here for the same reason it is published on the website: a vendor that only lists its wins is telling you nothing.

Item	Status
Independent penetration test	Planned — we will share the report and the remediation when it is done.
Scheduled backup-restore drill	Planned.
Nonce-based Content-Security-Policy	In progress.
SOC 2 or ISO 27001 certification	Not yet. We do not hold either, and we do not display badges for them.

We publish no target dates we cannot commit to. If one of these is a blocker for your procurement, tell us and it moves up the list.

Completing a security questionnaire? The technical-measures annex, the Privacy Impact Assessment and the Data Processing Agreement are in one pack — ask at security@carepath247.com and we will also fill in your own questionnaire, usually within a week.

Reporting a vulnerability? Email security@carepath247.com with what you found and how to reproduce it. Please give us a reasonable chance to fix it before publishing. We acknowledge within two business days.