PRIVACY & CLINICAL DATA GOVERNANCE

Privacy by design. Accountability by evidence.

Align eCare privacy and clinical data governance white paper

Design and governance position | 9 November 2026

Align eCare is developing a physician-controlled administrative execution and assurance layer for Canadian healthcare. This paper states its privacy commitments and the evidence required before a clinical deployment. It separates policy intent from implemented, independently assessed or contractually verified controls.

1. The commitments

- Patient and clinic information will never be used to train AI models.
- Clinical decisions and authorization remain with appropriately licensed professionals.
- Canadian data sovereignty is a design and deployment requirement.
- Information use must be limited to a defined, authorized workflow.
- Sources, uncertainty, responsibility and approval should remain visible.

What this paper establishes

It records product direction and deployment requirements. It does not establish a compliance certification, a completed security audit, a live integration or Canadian-only processing in a deployed clinical environment. The marketing website and its private preview are separate from the proposed clinical service.

INFORMATION FLOWS

Know the data.
Constrain the purpose.

2. Proposed clinical information flow

Authorized encounter and chart context → administrative preparation → evidence and completeness review → professional authorization → agreed routing → status and provenance.

Information category	Proposed purpose	Boundary to verify
Encounter audio or transcript	Support authorized preparation where recording is used.	Consent, recording controls, processor access and retention.
Chart context and supporting documents	Prepare the relevant form, referral or other task.	Source permissions, relevance, provenance and minimum required access.
Prepared administrative artifact	Present the exact content and destination for review.	Versioning, uncertainty and professional authorization.
Authorization and routing history	Show who approved what, when and for which destination.	Identity, access, event integrity and export behavior.
Patient handoff	Deliver clinician-approved instructions and next steps.	Recipient verification, channel, accessibility and disclosure.

3. No AI model training

The no-training commitment covers patient and clinic information. Enforcement must include the terms and settings of every processor that receives it. The deployment review must examine training, fine-tuning, evaluation, product improvement and human-access provisions rather than relying on a vendor slogan.

No training is not the same as zero retention. Processing, short-lived operational storage, required clinical records, logs and backups require their own defined purposes and retention rules.

PROCESSORS & PROFESSIONAL CONTROL

Canadian sovereignty. A verified chain.

4. Residency, sovereignty and third parties

A Canadian storage region alone does not demonstrate Canadian-only handling. Review primary storage, compute, logs, backups, failover, support access, subprocessors and relevant jurisdiction. Each vendor must have an identified role, authorized purpose, permitted access and documented obligations.

Control area	Evidence required before clinical processing
Hosting and processing	Inventory of locations, services, backups, failover and administrative access.
Subprocessors	Current list, roles, contracts, material-change process and flow-down restrictions.
Access controls	Roles, least privilege, identity, authentication, revocation and access review.
Retention and deletion	Schedules by information category; deletion, legal holds and backup handling.
Security and incident response	Threat review, safeguards, testing, monitoring, escalation and response responsibilities.

5. Physician authority and provenance

The proposed review surface identifies the patient and encounter, exact artifact, sources, checks, unresolved warnings, changes, destination and proposed action. Authorization must be bound to the approved version. The implementation should distinguish a prepared item from an approved item, a delivered transmission and a completed clinical task.

Biometric-backed approval, tamper-evidence and cryptographic envelopes remain implementation requirements. This paper does not assert that an immutable ledger, non-bypassable authorization or particular cryptographic control has been deployed.

DEPLOYMENT GATES

A clinical pilot needs more than a promise.

6. Minimum review gates

Gate	Review outcome
Workflow and scope	Name the clinic, information, purpose, task and excluded uses.
Legal roles and agreements	Establish responsibilities, applicable law, consent or authority, and processing terms.
Data and vendor evidence	Verify information flows, no-training terms, locations and subprocessors.
Security and privacy review	Complete the relevant impact and threat assessments and address identified gaps.
Clinical authorization tests	Demonstrate correct review, version binding, rejection and failure handling.
Retention and incident readiness	Approve category-specific schedules, access requests and incident procedures.
Pilot measurement	Define baseline, sample, measures, limits and reporting without overstating outcomes.

7. FHIR and integration boundaries

HL7 FHIR is a healthcare information-exchange standard. Its use does not itself establish privacy compliance, correctness or access to a vendor system. Confirm version, profiles, resources, permissions, data mapping, read/write scope and conformance tests for each connection.

No live EMR, pharmacy, CRA, portal or device connection is asserted by this white paper. Vendor names and regulatory references do not imply partnership, endorsement or approval.

OPENNESS & SOURCES

Clear status.
A route for questions.

8. Website and business enquiries

The public website explains the product and demonstrates synthetic workflows. Do not send patient records, appointment audio, identifiers or other health information to the business enquiry address. The private preview uses ChatGPT sign-in and hosting, which have separate service policies. Final public-host processing must be documented before public launch.

9. Review and contact

Before a clinical pilot, the evidence package should name the accountable privacy role, the authorized clinic contacts and the process for access, correction, deletion, complaints and incidents. Those deployment details are not established by this paper.

Business and governance enquiries: hello@alignecare.ca

Primary references

Office of the Privacy Commissioner of Canada. PIPEDA fair information principles. The principles address accountability, identified purposes, consent, collection and use limits, accuracy, safeguards, openness, access and complaints.

Read the OPC fair information principles

Office of the Privacy Commissioner of Canada. Accountability and safeguards guidance. These sources inform the proposed review gates; they do not certify Align eCare.

Read OPC accountability guidance

HL7 International. FHIR overview. Used to define the intended interoperability approach and its implementation boundaries.

Read the HL7 FHIR overview