

AuraScribe

Quebec-based AI Medical Documentation Platform

Privacy Policy

Version 2.0 • Effective 2026-05-01 • Last Updated: 2026-04-25

AuraScribe Inc. • 3200 Boulevard Cartier Ouest, Laval (Quebec) H7V 1J7, Canada

Privacy Officer: Salah Taieb, CEO • privacy@aurascribe.ca

Notice — Translation

The French version is the official version and takes precedence in the event of any discrepancy with this English translation.

⚙ Important Notice — AI Processing of Personal Health Information

AuraScribe processes consultation audio and clinical notes using artificial intelligence (AI) to generate structured medical documentation. This activity constitutes AI processing of personal health information as defined under Quebec's Law 25 and the Santé Québec PST (Technology Security Profile) requirements.

By accessing AuraScribe, healthcare professionals and their organizations expressly consent to AI processing (ai_processing) of their data as described in Section 5 of this Policy.

1. Introduction and Scope

AuraScribe Inc. ("AuraScribe", "we") is a Quebec-based AI-powered medical documentation platform that helps licensed healthcare professionals transcribe and document clinical consultations.

This Privacy Policy ("Policy") describes how we collect, use, retain, share, and protect personal information, including personal health information ("PHI"), in connection with our platform, APIs, and related services (collectively, the "Services").

This Policy applies to:

- Healthcare organizations, clinics, and establishments ("Organizations") that subscribe to AuraScribe;
- Physicians, nurses, and healthcare professionals ("Users") who access the platform; and
- Patients ("Data Subjects") whose information is processed as part of clinical documentation.

1.1 Applicable Legal Framework

Law	Scope
Law 25 (Quebec)	Protection of personal information in the Quebec private sector
PIPEDA	Protection of personal information in the Canadian private sector
AHSSS	Medical record retention, access to health information

Law	Scope
Public Health Act	Mandatory reportable diseases (MADO)
Professional Code	Obligations of healthcare professionals

2. Privacy Officer

In accordance with section 3.1 of Law 25, AuraScribe has designated a Privacy Officer (Responsable de la protection des renseignements personnels / RPRP):

Privacy Officer — AuraScribe Inc.

Salah Taileb, CEO

AuraScribe Inc., 3200 Boulevard Cartier Ouest, Laval (Quebec) H7V 1J7, Canada

Email: privacy@aurascribe.ca

Phone: available upon request

All privacy inquiries, rights requests, and concerns regarding the protection of personal information must be directed to the Privacy Officer.

3. Categories of Personal Information Collected

3.1 Account and Organizational Data

- **Organization data** : Name, address, professional license number, billing information, subscription tier.
- **User account data** : First and last name, professional title, RAMQ license number, email, role, preferences, access logs.

3.2 Patient Personal Health Information (PHI)

When a User initiates a consultation session, the following data may be collected and processed, with patient consent:

- **Consultation audio** : Audio recording of the consultation (processed in-memory by Deepgram Nova-3 only — not retained after processing).
- **Transcripts** : Raw speech-to-text output.
- **AI-generated clinical notes** : SOAP notes, referral letters, prescriptions, MADO forms, and other structured clinical documents.
- **Patient identifiers** : First and last name, date of birth, RAMQ / health insurance number, address, phone, email (to the extent provided by the User).
- **Medical data** : Diagnoses, medications, allergies, medical history, symptoms, lab results.
- **RAMQ billing codes** : Medical acts, diagnostic codes (ICD-10).

3.3 Technical and Usage Data

- IP address, browser type, operating system, device identifiers.
- Platform usage metrics (aggregated and de-identified form only).

- Audit logs: every access to PHI is recorded with user identifier, timestamp, action, and resource.

4. Legal Bases for Processing

Processing Activity	Legal Basis	Applicable Law
Account management and billing	Contractual necessity	Law 25, s. 12
Access to and processing of patient PHI	Informed patient consent	Law 25, s. 12; AHSSS
Transcription and clinical note generation	Consent (data_collection) + AI consent (ai_processing)	Law 25, s. 12
Sharing documents with other professionals	Consent (data_sharing)	Law 25, s. 12
Artificial intelligence processing	Explicit consent (ai_processing)	Law 25, s. 12; PST Santé Québec
Platform security and fraud prevention	Legitimate interest	Law 25, s. 12
Immutable audit logs	Legal obligation	Law 25, s. 12 (traceability)
RAMQ billing	Legal obligation	Health Insurance Act

SECTION 5 — AI Processing: Formal ai_processing Consent Type Disclosure (PST Santé Québec)

This section constitutes the formal ai_processing disclosure required under AuraScribe's PST framework and Law 25. It must be read carefully before using AI-powered documentation features.

5. Artificial Intelligence Processing (ai_processing)

5.1 Nature of AI Processing

AuraScribe uses machine learning models and large language models (LLMs) to perform the following activities:

- **Audio transcription** : Conversion of consultation audio to structured text (Deepgram Nova-3, in-memory processing, audio not retained).
- **Clinical note generation** : Automated drafting of SOAP notes, assessments, treatment plans, referral letters, and related documentation (Vertex AI Gemini, region northamerica-northeast1, Montreal).
- **Medical coding** : Suggestion of RAMQ billing codes and ICD-10 diagnostic codes.
- **Compliance monitoring** : Automated analysis of note structure and detection of residual PHI after generation (internal background task — results not shared with any third party).

5.2 Mandatory De-identification Before Any AI Call

No identifying data is transmitted to AI models

Before any call to Vertex AI or any other third-party model, AuraScribe's PHI Officer Agent systematically de-identifies all data: names, RAMQ numbers, dates of birth, addresses, and phone numbers are removed or replaced. Vertex AI therefore receives only de-identified transcripts.

5.3 AI Processing Consent (ai_processing)

The ai_processing consent is obtained separately:

- **User consent** : Obtained upon first activation of AI documentation features in account settings.
- **Patient consent** : Obtained by the Organization (clinic or establishment) before any recorded session, in accordance with AHSSS and Law 25.
- **Organizational consent** : Included in the data processing agreement signed with the Organization.

The ai_processing consent can be withdrawn at any time in Settings > Privacy > AI Processing Consent. Withdrawal disables AI note generation features but does not affect manual documentation.

5.4 AI Model Governance

- **Mandatory human review** : Every AI-generated note is presented to the clinician for review and approval before finalization. AuraScribe does not make autonomous clinical decisions.
- **No sale or sharing of AI-processed data** : Transcripts and generated notes are never sold, licensed for advertising, or shared with pharmaceutical, insurance, or research entities without explicit, separate consent.
- **No third-party model training** : Health data is never used to train general-purpose AI models by sub-processors.
- **Model improvement feedback (opt-in only)** : Contributing corrected notes for model improvement is strictly optional, separate from the base ai_processing consent, and never assumed.

6. Data Sharing

We do not sell personal information. We share data only in the following circumstances:

Recipient	Data Shared	Legal Basis
Vertex AI (Google Cloud)	De-identified transcripts only	Google Cloud DPA; northamerica-northeast1
Deepgram	Consultation audio (in-memory, not retained)	Deepgram DPA
OVH Canada	Encrypted infrastructure (no data access)	OVH hosting agreement
Stripe	Tokenized payment references (no health data)	Stripe DPA
Quebec EMRs (Omnimed, KinLogix, etc.)	Exported clinical documents, at User instruction	User consent + Organization instruction

Recipient	Data Shared	Legal Basis
Legal authorities	Under court order or legal obligation, with notice where permissible	Legal obligation
Successor entity in business transfer	Subject to equivalent protections and prior notice	Law 25, s. 18.4

Data Residency — 100% Canada

No health data leaves Canada. All infrastructure is hosted in Beauharnois, Quebec (OVH BHS) and Montreal (GCP northamerica-northeast1).

7. Data Retention and Destruction

Category	Period	Legal Reference
Medical record (transcripts, SOAP notes)	10 years	AHSSS
MADO forms	50 years	Public Health Act
Audit logs	7 years	Law 25, s. 12
Consent records	20 years	Extended legal protection
RAMQ billing data	7 years	Income Tax Act
User account data	7 years post-termination	Law 25
Consultation audio	Not retained (in-memory processing only)	Data minimization
Security logs	7 years	Law 25, s. 12

Soft delete: All PHI tables use logical deletion — records are marked as deleted but retained to satisfy regulatory retention obligations. Physical destruction is performed by an automated retention scheduler upon expiry of applicable periods.

Anonymization: Upon expiry of retention periods, data is irreversibly anonymized in accordance with section 23 of Law 25 before any destruction.

8. Security of Personal Information

Measure	Implementation
Encryption at rest	AES-256-GCM at the field level for every PHI-bearing column
Encryption in transit	TLS 1.3 on all client-server and inter-service communications
Authentication	JWT (15 min) + rotating refresh tokens with reuse detection
Mandatory MFA	TOTP (RFC 6238) required for all User accounts

Measure	Implementation
Access control	RBAC (owner / admin / physician / nurse) + multi-tenant isolation at database level
Audit logs	Immutable, append-only; all PHI access traced
Secret management	GCP Secret Manager in production — no secrets hardcoded
Breach detection	Automated hourly analysis of access anomalies
Rate limiting	Per-IP and per-user rate limiting on all sensitive endpoints
Penetration testing	External penetration testing conducted before large-scale production rollout

8.1 Privacy Incidents

In the event of a privacy incident presenting a serious risk, AuraScribe will:

- Notify the Commission d'accès à l'information (CAI) within 72 hours of discovering the incident, in accordance with section 3.5 of Law 25.
- Notify affected Organizations (subscribed clinics) as soon as possible.
- Notify affected individuals when the risk is serious, in accordance with section 3.5 of Law 25.

To report a security incident: security@aurascribe.ca

9. Rights of Individuals

In accordance with sections 27 and 28 of Law 25 and sections 8 et seq. of PIPEDA, you have the following rights regarding your personal information:

Right	Description	Deadline
Right of access (Law 25, s. 27)	Obtain a copy of the personal information we hold about you	30 days
Right to rectification (Law 25, s. 27)	Request correction of inaccurate or incomplete information	30 days
Right to erasure (Law 25, s. 28)	Request deletion of information collected without valid legal basis, subject to legal retention obligations	30 days
Right to data portability (Law 25, s. 27)	Receive your data in a structured, machine-readable format	30 days (automated)
Withdraw ai_processing consent	Withdraw ai_processing consent at any time	Immediate
Right to information	Know the categories of data held and their use	Available at all times
Right to file a complaint	File a complaint with the CAI if you believe your rights have not been respected	—

To exercise your rights: Submit a request to privacy@aurascribe.ca or through the rights request portal accessible from the platform. We acknowledge receipt within 5 business days and respond within 30 days (extendable by 30 additional days for complex requests, with prior notice).

Patient data rights: Rights requests relating to patient health data should first be directed to the Organization (clinic or establishment), which is responsible for the medical record. AuraScribe cooperates with Organizations to facilitate such requests.

Recourse — Commission d'accès à l'information (CAI)

If you are not satisfied with our response, you may file a complaint with the CAI:
www.cai.gouv.qc.ca • 1 888 528-7741

10. Consent and Consent Management

AuraScribe manages three distinct consent types in accordance with Law 25, section 12:

Type	Purpose	Obtained By
data_collection	Collection of personal health information	Organization (clinic) from the patient, before each session
data_sharing	Sharing with other professionals or establishments	Organization, patient consent required
ai_processing	Processing by artificial intelligence	User (clinician) via the platform + Organization via the data processing agreement

Each consent is recorded with: type, date, method of collection (verbal, written, electronic), policy version, identifier of the professional who collected the consent.

Consents may be withdrawn at any time. Withdrawal does not affect the lawfulness of processing carried out before withdrawal.

11. Cookies and Tracking Technologies

Category	Purpose	Disableable
Essential	Session management, authentication, security	No (disabling prevents platform access)
Functional	User preferences (language, theme)	Yes
Analytics	De-identified platform usage metrics	Yes (no functional impact)

We do not use advertising cookies or third-party trackers for commercial targeting. Preferences can be managed via the Cookie Preferences Centre accessible from the platform.

12. Changes to This Policy

We may update this Policy at any time. Material changes — particularly those affecting AI processing or the categories of data subject to ai_processing — will be communicated to subscribed Organizations:

- By email to the designated privacy contact of each Organization at least 30 days before the change takes effect; and
- By in-platform notification to all active Users.

Where a material change requires fresh ai_processing consent, that consent will be sought before the change takes effect.

13. Contact Us

Contact — AuraScribe Inc.

Privacy Officer: privacy@aurascribe.ca

Security incidents and breach reporting: security@aurascribe.ca

General inquiries: hello@aurascribe.ca

Mailing address: AuraScribe Inc., 3200 Boulevard Cartier Ouest, Laval (Quebec) H7V 1J7, Canada

AuraScribe Privacy Policy — Version 2.0 — Effective 2026-05-01

This document satisfies the ai_processing consent type disclosure requirements of the Santé Québec PST and the obligations of Quebec Law 25.