

PreVisit

Data Processing Agreement

Agreement governing the processing of personal health information on behalf of clinics

Version 1.0 · Effective: March 27, 2026 · Jurisdiction: British Columbia, Canada

This Data Processing Agreement ("DPA") is entered into between the subscribing clinic or clinician ("Controller") and PreVisit ("Processor"). This DPA forms part of and is incorporated into the Clinician User Agreement. In the event of any conflict, this DPA governs with respect to the processing of personal information.

1. Definitions

- **"Controller"**: The clinic or clinician that determines the purposes and means of processing Patient Data
- **"Processor"**: PreVisit, which processes Patient Data on behalf of the Controller
- **"Personal Information"**: Personal information about an identifiable individual collected via the PreVisit intake form
- **"Subprocessors"**: Third-party organizations engaged by PreVisit to process Personal Information (see Schedule A)
- **"PIPA BC"**: The Personal Information Protection Act (British Columbia) SBC 2003, c. 63
- **"Privacy Breach"**: A breach of security safeguards leading to unauthorized access, disclosure, or loss of Personal Information

2. Scope and Purpose of Processing

PreVisit processes Personal Information solely for the purpose of providing the Service to the Controller — specifically, to receive patient intake responses, generate AI-assisted SOAP Notes, deliver those notes to the Controller, and store submission records as directed.

PreVisit processes the following categories of Personal Information:

- Health history and symptom information provided by Patients via the intake form
- Self-reported medications, allergies, and vitals (blood pressure, heart rate, height, weight)
- Submission metadata (date, time, complaint category)

Restrictions: PreVisit will not process Personal Information for any purpose other than providing the Service, unless required by law. PreVisit will not sell, rent, or share Personal Information with third parties for their own purposes.

3. Controller Obligations

The Controller represents and warrants that it:

- Has a lawful basis for collecting and directing the processing of Patient Data under PIPA BC
- Has provided Patients with appropriate notice of the use of PreVisit (e.g., via the Patient Intake Disclosure)
- Has obtained any consent required by applicable law or professional standards
- Is responsible for ensuring that Patient Data submitted to PreVisit is accurate
- Will comply with all applicable privacy legislation in its use of the Service

4. Processor Obligations

PreVisit agrees to:

- Process Personal Information only on documented instructions from the Controller
- Ensure personnel authorized to process Personal Information are bound by confidentiality obligations
- Implement and maintain reasonable technical and organizational security measures (see Section 5)
- Assist the Controller in responding to individual rights requests under PIPA BC
- Notify the Controller of any Privacy Breach in accordance with Section 7
- Delete or return Personal Information upon termination as described in Section 8
- Provide information necessary for the Controller to demonstrate compliance with applicable law

5. Security Measures

PreVisit implements the following security measures to protect Personal Information:

- All data in transit is encrypted using TLS 1.2 or higher
- All data at rest is encrypted using AES-256 or equivalent
- Access to Personal Information is restricted to authorized personnel on a need-to-know basis
- Authentication controls are enforced for all personnel accessing Personal Information
- Regular security reviews are conducted of our technical infrastructure
- Subprocessors are assessed for their security practices prior to engagement

PreVisit will review and update these measures as technology and risk evolve. The Controller acknowledges that no security system is impenetrable and that PreVisit cannot guarantee absolute security of Personal Information.

6. Subprocessors

The Controller authorizes PreVisit to engage the Subprocessors listed in Schedule A to process Personal Information as necessary to provide the Service. PreVisit will ensure each Subprocessor is bound by data protection obligations no less protective than those in this DPA.

Changes to Subprocessors: PreVisit will notify the Controller at least 14 days before engaging a new Subprocessor or making material changes to existing Subprocessors. The Controller may object to such changes by notifying PreVisit in writing within 14 days.

7. Privacy Breach Notification

In the event of a Privacy Breach affecting Personal Information processed under this DPA, PreVisit will notify the Controller without undue delay and in any event within 72 hours of becoming aware of the breach. Notification will include:

- A description of the nature of the breach
- The categories and approximate number of individuals affected
- The categories and approximate volume of Personal Information affected
- Likely consequences of the breach
- Measures taken or proposed to address the breach

Controller responsibility: The Controller is responsible for determining whether and how to notify affected individuals and the Office of the Information and Privacy Commissioner for BC (OIPC) in accordance with PIPA BC.

8. Data Retention and Deletion

Personal Information is retained for as long as the Controller's subscription is active and for such additional period as required by applicable law. Upon termination of the Clinician User Agreement, PreVisit will, at the Controller's election:

- Delete all Personal Information within 90 days of termination, or
- Return Personal Information to the Controller in a standard machine-readable format

Aggregated data: PreVisit may retain de-identified, aggregated data derived from Personal Information for service improvement purposes, provided that such data cannot be used to identify any individual.

9. Individual Rights Requests

If PreVisit receives a request directly from a Patient to access, correct, or delete their Personal Information, PreVisit will promptly forward the request to the Controller. PreVisit will assist the Controller in fulfilling such requests to the extent reasonably practicable and in accordance with PIPA BC.

10. Cross-Border Data Transfers

Personal Information may be transferred to and processed in jurisdictions outside British Columbia, including the United States, where PreVisit's Subprocessors operate (see Schedule A). The Controller acknowledges and consents to such transfers as necessary to provide the Service.

Clinics with residency requirements: PreVisit will ensure that any cross-border transfer is made with appropriate safeguards in place. Clinics subject to FIPPA or with specific data residency requirements should contact PreVisit at noreply@previsit.ca before activating the Service.

11. Audit Rights

The Controller may request, no more than once per year and with 30 days written notice, a summary of PreVisit's security practices and Subprocessor list. PreVisit will provide reasonable documentation to demonstrate compliance with this DPA. On-site audits require mutual agreement and are subject to reasonable confidentiality obligations.

12. Term and Termination

This DPA is effective for the duration of the Clinician User Agreement. Obligations relating to Personal Information already processed survive termination until that information is deleted or returned in accordance with Section 8.

13. Governing Law

This DPA is governed by the laws of British Columbia and the federal laws of Canada applicable therein, including PIPA BC. Nothing in this DPA limits either party's obligations under applicable privacy legislation.

SCHEDULE A — APPROVED SUBPROCESSORS

The following Subprocessors are currently engaged by PreVisit to process Personal Information:

Subprocessor	Location	Purpose	Website
Anthropic (Claude API)	United States	AI SOAP note generation from patient intake data	anthropic.com
Supabase	United States	Secure database storage of submissions and SOAP notes	supabase.com
Railway	United States	Backend application hosting (FastAPI server)	railway.app
Resend	United States	Transactional email delivery of SOAP notes to clinicians	resend.com

Note: This list will be updated as Subprocessors change. Updates will be communicated to Controllers in accordance with Section 6 of this DPA.

