

Sera

Security & Compliance

Last updated: 28 October 2026

This page describes how Sera protects your data and your clients' data, the sub-processors we rely on, the cross-border transfer mechanisms we use, and the regulatory frameworks we operate under. It is intended to be readable by practitioners, their compliance officers, and their regulators.

For questions not answered here, contact us at transcendentalia@gmail.com.

Find your country. The sections that apply where you practise:

- **United Kingdom:** UK and EU GDPR; International data transfers
- **European Union:** UK and EU GDPR; International data transfers
- **Canada:** PIPEDA; PHIPA (Ontario); International data transfers
- **United States:** HIPAA

How your data is protected

Sera treats practitioner accounts and client health data as sensitive by default. The following controls are always on:

- **Encryption at rest.** All data in Sera's Postgres database is encrypted at rest by our database provider (Neon) using AES-256.
- **Encryption in transit.** All connections to Sera use HTTPS/TLS. HSTS is enforced by Vercel.
- **Workspace isolation.** Every database query is scoped to the practitioner's account. No practitioner can read another practitioner's clients or results.
- **Password hashing.** Account passwords are hashed with bcrypt (cost factor 12). Plain-text passwords are never stored.
- **Server-side consent enforcement.** Account creation is refused server-side if consent to Terms of Service and Privacy Policy is not provided. Consent is recorded with policy version, timestamp, and IP address for audit.
- **Access restriction.** Access to the production database is restricted to what is needed to operate Sera. Sera's founder has admin access and does not access practitioner data outside of investigating specific issues raised by the practitioner.

Sub-processors

Sera uses three sub-processors to operate. Each is covered by a Data Processing Agreement (DPA) incorporated into our agreement with them, and is bound by our privacy commitments.

- **Neon** — PostgreSQL database. Data stored: everything you enter into Sera (account, clients, sessions, biomarker entries, interventions, notes, consent records, activity records, diagnostic events).
- **Vercel** — application hosting, serverless functions and file storage. Data processed: request traffic, session tokens, temporary in-memory processing during request handling. Data stored: the lab report PDFs kept with saved blood tests, and the test report PDFs you add to a client's Tests tab, in a private, encrypted file store, deleted with the blood test or test, the client or your account.
- **Anthropic** — Claude API used for PDF parsing. Data processed: the extracted text of uploaded lab report PDFs (not the PDF file itself). Under Anthropic's commercial API terms, this data is not used to train Anthropic's models and is retained by them only for a limited period to operate the service and guard against misuse.

The DPAs covering all three sub-processors are available on request.

International data transfers

All three of Sera's sub-processors operate from the United States. This means that data belonging to UK, EU, and Canadian practitioners and their clients is transferred outside the UK, EEA, and Canada.

These transfers are made lawful by the Standard Contractual Clauses (SCCs) included in our Data Processing Agreements with each sub-processor:

- Neon — SCCs in Neon's DPA
- Vercel — SCCs in Vercel's DPA
- Anthropic — SCCs in Anthropic's commercial terms

SCCs are the primary and legally sufficient transfer mechanism under UK GDPR and EU GDPR. They provide the legal basis for the transfer and are recognised by the European Commission and the UK Information Commissioner's Office.

United Kingdom and European Union — GDPR

Sera operates under UK GDPR (as retained in UK law) and EU GDPR.

Framework. Sera operates as a **processor** of client health data on behalf of practitioners. The practitioner is the **controller** — they decide what data to record about clients and are responsible for obtaining client consent, responding to client access and correction requests, and notifying clients of breaches. Sera provides the export and delete tools practitioners need to fulfil these obligations.

Legal basis for processing (GDPR Article 6):

- Contract performance — for account operations, authentication, storing your workspace, parsing lab reports.
- Legitimate interest — for securing the service, error logging, understanding how Sera is used from sign-ins and pages opened, and reviewing unrecognised biomarker names and units so we can support more laboratories.
- Consent — for anything beyond what is needed to operate the service, recorded with policy version when you register.

Data subject rights are available to every user under GDPR:

- Access — everything you enter is visible to you in the app at any time. Consent, activity, diagnostic and upload records are not shown on a screen, but are included in full in the JSON export.
- Rectification — correct your account information from Settings; edit client records directly in the workspace.
- Portability — export all of your workspace data as a single JSON file from Settings.
- Erasure — permanently delete your account and all associated data from Settings. Diagnostic event records are the one exception: they are retained for the remainder of their 90-day window with your account no longer named on them.
- Restriction — ask us to temporarily limit processing while a dispute is being resolved (contact transcendentalia@gmail.com).
- Objection — object to processing based on legitimate interest (contact transcendentalia@gmail.com).

Breach notification. In the event of a personal data breach likely to result in a risk to your rights or your clients' rights, we will notify you without undue delay and notify the relevant supervisory authority within 72 hours as required by GDPR Article 33. Sera has no email or in-app notification channel at present, so notice to you will be published on this page and sent by any means of contact we hold for you. Our Incident Response Plan v1.0 (filed 12 September 2026) documents the process.

Data Protection Authority complaints. You have the right to lodge a complaint with:

- **United Kingdom:** Information Commissioner's Office (ico.org.uk)
- **European Union:** Your national data protection authority

Canada — PIPEDA

Sera operates under the Personal Information Protection and Electronic Documents Act (PIPEDA) for Canadian practitioners and clients.

Framework. As with UK/EU GDPR, Sera acts as a processor on behalf of the practitioner. The practitioner is responsible for obtaining meaningful consent from clients, handling access and correction requests, and providing PIPEDA-compliant privacy practices to their own clients.

Purposes for collection. Sera collects personal information for these specific purposes:

- Authentication (email, hashed password)

- Client record keeping (name, biological sex, full date of birth, notes)
- Health data storage and analysis (biomarker values, panel dates, session notes, menstrual cycle day where relevant)
- Intervention tracking (supplements, medications, diet, lifestyle changes logged by the practitioner)
- Diagnostic and operational logs (error events, upload attempts, consent records)
- Activity (sign-in times and which pages of Sera were opened, kept 90 days; no IP address, device, or page contents)

Accountability. Alina Radu is the individual designated as accountable for Sera's compliance with PIPEDA (Principle 4.1). Contact for privacy questions and data subject requests: transcendentalia@gmail.com.

Cross-border transfer disclosure. Data is transferred to the United States for storage and processing. This is disclosed to you at signup via the Privacy Policy and is authorised by Standard Contractual Clauses in our DPAs. See "International data transfers" above.

Breach notification. In the event of a breach that poses a real risk of significant harm, Sera will notify affected practitioners and, as required by PIPEDA, notify the Office of the Privacy Commissioner of Canada.

Complaints. You have the right to complain to the Office of the Privacy Commissioner of Canada (priv.gc.ca).

Ontario — PHIPA

For practitioners in Ontario using Sera to store personal health information (PHI) within the meaning of the Personal Health Information Protection Act (PHIPA), Sera acts as your **agent** under Section 17 of PHIPA.

Written agreement. These Terms of Service and this Security & Compliance page together constitute the written agreement between you (the health information custodian) and Sera (as your agent).

Sera's PHIPA commitments as your agent:

- Collect, use, disclose, retain, and dispose of PHI only as permitted by you and required by PHIPA.
- Provide reasonable safeguards — encryption at rest and in transit, workspace isolation, access restrictions — as described in "How your data is protected" above.
- Notify you at the first reasonable opportunity if PHI in Sera is stolen, lost, or used or disclosed without authorisation.
- Assist you, on request, in fulfilling your obligations under PHIPA to respond to client access and correction requests.

Your PHIPA responsibilities as the health information custodian:

- Obtain consent from clients as required by PHIPA.
- Respond to client requests for access to or correction of their PHI.
- Notify the Information and Privacy Commissioner of Ontario of breaches as required by PHIPA Section 12(3).
- Notify affected individuals of breaches as required by PHIPA.

Complaints. Ontario clients may complain to the Information and Privacy Commissioner of Ontario (ipc.on.ca) for matters relating to their PHI.

This section applies in addition to, and does not replace, the UK/EU GDPR processor framework and the PIPEDA framework above.

United States — HIPAA

Sera is **not currently HIPAA-compliant** and should not be used by US healthcare practitioners to store Protected Health Information (PHI) within the meaning of HIPAA. Sera does not sign Business Associate Agreements.

Whether HIPAA applies to you. HIPAA applies to covered entities (health plans, healthcare clearinghouses, and healthcare providers who send health information electronically in connection with standard transactions such as billing a health plan) and to their business associates. Whether your practice is a covered entity is for you and your adviser to determine. The US Department of Health and Human Services publishes guidance at hhs.gov. If HIPAA applies to your practice, do not enter your clients' identifiable health information into Sera.

HIPAA compliance is on our roadmap as a paid tier for US practitioners. Practitioners who would like to be notified when a HIPAA-compliant tier becomes available can register their interest by emailing transcendentalia@gmail.com.

Until then, US practitioners are welcome to use Sera for personal use, training data, non-PHI review, or scenarios where the data is not covered by HIPAA— but Sera cannot be used to store the PHI of US patients.

What Sera does not do

- We do not sell, share, or monetise your data in any way.
- We do not show advertisements.
- We do not use tracking pixels or third-party advertising analytics.
- We do not use your clients' health data to train AI or machine learning models, and our AI provider does not either.
- We do not build advertising profiles about you or your clients.
- We do not access practitioner data outside of investigating specific issues raised by the practitioner.

Supporting documents

For deeper detail, see:

- Privacy Policy — the full published policy applied to your account
- Terms of Service — including the PHIPA agent agreement in Section 9

The DPAs covering our sub-processors (Neon, Vercel, Anthropic) are available on request.

Contact

Alina Radu is the person accountable for Sera's privacy and security practices.

- General questions, data subject requests, or compliance inquiries: transcendentalia@gmail.com
- Security incident reports: transcendentalia@gmail.com with subject "Security Incident Report" for priority handling