Eluve security & compliance, on one page.

Everything your IT, security, or compliance reviewer needs to clear Eluve for use: the leave-behind a clinician can forward. Deeper documentation (SOC 2 report, BAA, subprocessor list, architecture) is available on request under NDA.

HIPAA compliant | **PIPEDA compliant** | **SOC 2 Type I & II** | **Pursuing HITRUST** | **BAA available** | **AMA CPT® licensee**

Data protection

- Encryption in transit and at rest.
- Data retention is governed by the BAA and Privacy Policy.
- No cross-customer data mixing; strict tenant isolation.
- AI models are trained only on de-identified data, never on identifiable PHI, as permitted under the BAA.

Compliance & certifications

- HIPAA (US) and PIPEDA (Canada) compliant.
- SOC 2 Type I & Type II certified; pursuing HITRUST.
- Business Associate Agreement (BAA) available for every practice.
- Independently audited by third parties on a regular cadence.

Access & identity

- Role-based access control (RBAC): least-privilege by default.
- SSO / SAML supported for enterprise identity.
- Audit logs for every artifact and action.
- Full clinical provenance: every output is traceable.

Deployment & integration

- Cloud or customer VPC deployment.
- Regional data residency available.
- EHR integration via HL7v2, FHIR, and REST.
- Clinician reviews and approves every note before it enters the record.

Monitoring & oversight

- 24/7 system monitoring and alerting.
- Red-team testing and bias evaluations.
- Clinician-in-the-loop by design: Eluve supports, never replaces, clinical judgment.
- Documented incident-response and vulnerability-management processes.

Full report & BAA available on request: privacy@eluve.com

eluve.com/platform/security