



Your feeds. Our checks.

Trestl collects claims from the systems you already run, checks them before payment, and returns the results the same way. No software to install. Each client's data is walled off, encrypted and hosted in the US, and we will walk your security team through the evidence.



The Trestl Exchange

- A **per-client** set of connectors for data in and results out, isolated by tenant.
- **Inbound:** claims, member and enrollment files, and plan configuration.
- **Outbound:** claim results in CSV or JSON, with a status and reason for every claim.
- Every run and file **recorded**, from detection through validation to archive.

Before any real data moves

- We agree the permitted purpose, the minimum necessary fields, the route, retention and the agreements that apply.
- The route, file contract and schedule are tested with a representative file before any live data is sent.
- Data is processed only to deliver the agreed service, and returned or destroyed when the agreement ends.

How your data is protected

- **Tenant isolation that fails closed:** row-level security; a request without a valid client context sees no rows.
- **Encryption:** TLS in transit; data encrypted at rest, with keys in Google Cloud KMS on scheduled rotation.
- **Least-privilege access:** single sign-on, roles scoped to each client, sign-out after 30 minutes idle.
- **Tamper-evident audit trail:** access to claims data and admin actions, in an append-only, hash-chained ledger verified daily.
- **Hosted in the US:** Google Cloud US regions, enforced by an organization policy.
- **Monitoring:** detections open incident records, backed by a documented response plan.
- **AI checks** run on Vertex AI inside our Google Cloud BAA; claims data is not used to train models.

What we have, and what we do not claim

- **HIPAA:** where we handle protected health information for you, we sign a business associate agreement before any of it is exchanged; our cloud provider's BAA covers the services we use.
- **SOC 2:** controls mapped to the Trust Services Criteria are implemented and monitored. An independent attestation is on our roadmap; we do not claim one today.
- **NAIC:** controls mapped to the Insurance Data Security Model Law (MDL-668).
- **Testing:** an annual penetration test, findings tracked to remediation; the 2026 test was in-house, an independent test is planned. Dependencies and images are scanned continuously.

Found a security issue?

Email security@trestlsolutions.com, subject "Security", with steps to reproduce. Don't access, change or keep data beyond what shows the issue; don't exploit it or disrupt the service; stop if you reach personal or health information; and give us reasonable time to fix it before disclosing it. We reply within two business days, update you within ten, and don't pursue good-faith researchers who follow these steps.

BAA available

Encrypted in transit and at rest

Tenant-isolated

US-hosted

Tamper-evident audit trail

Supported routes, formats and schedules are confirmed for each environment in the interface agreement and partner testing. Bring your security questionnaire: we walk your team through our controls, policies and evidence during discovery. © 2026 Trestl Health Solutions, LLC.

