Protocol Wealth - Privacy, Security & Compliance Posture

Public snapshot - 2026-06-11

Effective: 2026-06-11
Owner: Nick Rygiel (CTO/CISO)

Protocol Wealth LLC is an SEC-registered investment adviser (CRD #335298). This page summarizes how we protect client information, operate our AI-assisted advisory stack, supervise service providers, and preserve required records.

This is a public summary, not an exhaustive control report, SOC 2 report, ISO certificate, or replacement for our client agreements, Form ADV, Privacy Notice, or other required disclosures. We state material limitations plainly because public security communications should be fair, balanced, and verifiable.

Core Commitments

- We do not sell client information.
- Client data is not used to train AI models.
- Client data is processed on United States infrastructure for our primary systems and primary AI inference path.
- Access to client data is role-restricted, logged, and reviewed through our security and compliance program.
- Client-facing AI-assisted work remains subject to human adviser review and fiduciary judgment.
- Required advisory records are retained under the firm's books-and-records program.

Privacy and AI Controls

Protocol Wealth uses AI as an adviser-assistance tool, not as an unsupervised decision maker. AI helps with research, monitoring, summarization, and document preparation. Final investment decisions, fiduciary advice, and client-facing communications remain with a human adviser.

Our primary reasoning-model provider is Anthropic's Claude API under a formally approved Zero Data Retention configuration. Under that arrangement, our API inputs and outputs are not retained for model training or model improvement, and inference for that primary path is restricted to US-based infrastructure.

We also use two narrow AI capabilities:

- Google Gemini API for adviser-facing image and graphics generation.
- OpenAI Whisper for adviser-initiated voice-memo transcription.

Those narrow services are disclosed in our Subprocessors Inventory and are not used as general client-advice engines.

We maintain a schema-level PII tagging model (`pii.high`, `pii.medium`, `pii.low`) and a PII egress guard designed to prevent high-risk identifiers from being sent to AI systems. High-risk fields include government identifiers, full account numbers, private keys, seed phrases, biometric data, and authentication artifacts. We also keep an independent egress canary at AI call sites so residual PII detection can block a request before it leaves our environment.

Data Security Controls

Protocol Wealth runs production workloads primarily on Google Cloud Platform.

Key controls in place:

- **Encryption in transit:** external traffic uses TLS 1.2 or better, with TLS 1.3 preferred.
- **Encryption at rest:** Cloud SQL and Cloud Storage data are encrypted at rest with AES-256 using Google-managed keys. Sensitive vendor credentials receive an additional application-layer AES-256-GCM envelope and are decrypted only in memory.
- **Tenant isolation:** client data is isolated by database-enforced row-level security, not only by application convention.
- **Private data services:** production Cloud SQL and Redis services are private-network-only.
- **Authentication:** multi-factor authentication is required for client and adviser surfaces; newer client onboarding uses passkey-first authentication.
- **Least privilege:** service access is scoped by role and workload identity. Long-lived service-account keys are disabled by organization policy.
- **Audit logging:** state-changing actions write to a canonical audit log and are retained under the firm's records program.
- **WORM retention:** audit records mirror to a retention-locked Google Cloud Storage archive for seven years.
- **Monitoring:** cloud-configuration-change alerts, Google Security Command Center findings, dependency scanning, code scanning, and PII-egress alerts feed operational security review.

Incident Response and Recordkeeping

Protocol Wealth maintains a written incident response plan covering detection, containment, investigation, recovery, post-incident review, and customer notification. Under amended SEC Regulation S-P, the firm commits to notifying affected customers as soon as practicable and no later than

30 days after becoming aware that sensitive customer information was accessed or used without authorization, subject to the rule's limited exceptions.

Advisory books and records are retained under the firm's Rule 204-2 program. Audit records are retained for seven years as a conservative baseline. Electronic records that must be preserved are protected from alteration or deletion for the required retention period.

Vendor and Subprocessor Oversight

Protocol Wealth reviews service providers before onboarding and on a recurring basis. The public Subprocessors Inventory identifies material vendors, their role, data categories, and relevant security attestations where available.

Representative categories include:

- Cloud infrastructure and internal collaboration.
- AI services.
- Identity verification and sanctions screening.
- Account aggregation.
- Custody, brokerage, and digital-asset infrastructure.
- CRM, communications, and document-signing services.

Account aggregation currently operates through Quiltt and its data-provider network. If Protocol Wealth enables an additional client-facing data provider, the Privacy Policy, Subprocessors Inventory, consent flow, and client-facing disclosures will be updated before client use.

Self-Custodial Digital Assets

For clients who hold crypto, Protocol Wealth has built a self-custodial wallet model where the client is intended to remain the signing authority and Protocol Wealth is structurally unable to move client crypto.

The model uses client-held passkeys and a fail-closed provisioning check that prevents a wallet from becoming active if Protocol Wealth is in the signing quorum. Protocol Wealth may assist with recovery workflows, but the recovery helper is non-root and policy-restricted.

Current status: the production custody path has passed live acceptance testing, including a real wallet provisioning and passkey ceremony. Broader client rollout remains controlled and subject to per-client adviser, compliance, and operational gates.

Compliance Framework

Protocol Wealth's security program is designed around the firm's obligations as an SEC-registered investment adviser, including Regulation S-P, Rule 204-2 books and records, fiduciary supervision, and Marketing Rule review for public communications.

The firm also maintains an ISO/IEC 27001:2022-aligned Information Security Management System, including a Statement of Applicability and Risk Register. This is an internal control framework and diligence artifact. Protocol Wealth is **not** ISO 27001 certified.

Protocol Wealth does **not** currently hold a firm-level SOC 2 report. We rely on vendor SOC 2 reports where appropriate and maintain a readiness path in case a future customer, partner, or commercial need justifies a firm-held SOC 2 engagement.

Where FINRA standards are relevant through broker-dealer partners or public communications discipline, we draft communications to be fair, balanced, and not misleading. Protocol Wealth does not present this document as a FINRA member communication unless separately approved through the appropriate channel.

Current Limitations and Roadmap Items

The following are not claims of completed controls:

- Customer-managed encryption keys (CMEK) and column-level field encryption are approved hardening items but are not yet in production.
- A formal external penetration test is planned but not yet completed.
- Periodic access-review cadence and just-in-time custom roles are being matured.
- The independent PII egress canary is being extended across remaining API egress paths.
- ISO 27001 certification and firm-level SOC 2 are not current claims.

Verification and Contact

Qualified partners and institutional reviewers may request additional diligence materials under appropriate confidentiality terms, including vendor due-diligence evidence, anonymized audit-log samples, the ISO-aligned Statement of Applicability, the Risk Register, and security-policy artifacts.

- Privacy and compliance: `compliance@protocolwealthllc.com`
- Security and vulnerability disclosure: `security@protocolwealthllc.com`
- Form ADV Part 2A: `adviserinfo.sec.gov/firm/brochure/335298`

Protocol Wealth, LLC | SEC-Registered Investment Adviser | CRD #335298