

Protocol Wealth - Privacy, Security & Compliance Posture

Public security summary

Effective: 2026-09-25

Owner: Adam Blumberg (CCO) + 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, oversee service providers, and preserve required records.

Classification: Public. Dated snapshot. It describes our practices as checked on the date above. It is not a promise about any later date. Re-verify before sending it to anyone.

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

What We Do

- We do not sell client information.
- Our AI providers' terms exclude our data from model training.
- Our primary systems, and our primary AI provider's inference, run on United States infrastructure.
- Access to client data is limited by role, and actions that create, change or delete client data are written to an audit log.
- A human adviser remains responsible for advice. Recommendations and client communications are reviewed by an adviser before they reach a client. The one exception is the AI assistant in the client portal, described below.
- 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 communications remain with a human adviser.

- **Anthropic (Claude API)** is our primary AI provider. It is engaged under a Zero Data Retention agreement, with inference restricted to U.S. infrastructure.
- **xAI (Grok)** is a second model that advisers can choose in advisor chat, available since September 22, 2026.
 - xAI is engaged under team-level zero data retention.
 - Our systems check xAI's retention assertion on every response. The check runs after the request is sent.
 - Requests go only to xAI's U.S. regional endpoints.
- **Google Gemini, through Google Cloud's Vertex AI:** adviser-facing image and graphics generation, and search indexing of documents added to advisor chat. Since September 23, 2026, requests go to Vertex AI's U.S. endpoints.
- **OpenAI:** drafting of the firm's non-client material. We do not send OpenAI client records.
- **The AI assistant in the client portal** is a limited beta that runs on Claude.
 - It answers a client's questions about their own accounts, and general educational questions.
 - It does not give investment advice or recommendations, and it does not trade, move money or change accounts.
 - Its answers are shown to the client directly, without adviser review.

Before text is sent to an external AI provider, our systems replace the identifiers they recognize with placeholders. Those include government identifiers, account numbers, email addresses, phone numbers and dates of birth. Recognition is by pattern and is not complete. **It does not remove names.** An independent egress check can block a request that still carries recognized structured identifiers. The AI providers and what each receives are listed in our Privacy Policy and List of Subprocessors.

Data Security Controls

Protocol Wealth runs production workloads primarily on Google Cloud Platform.

- **Encryption in transit:** our public endpoints accept TLS 1.2 or higher, and refuse TLS 1.0 and 1.1. We checked this on September 25, 2026 for pwos.app, pwportal.app, webhooks.protocolwealthllc.com and protocolwealthllc.com.
- **Encryption at rest:** Cloud SQL and Cloud Storage data are encrypted at rest with Google-managed keys (AES-256). Sensitive vendor credentials get an additional application-layer AES-256-GCM envelope and are decrypted only in memory. Customer-managed encryption keys (CMEK) are not in place.
- **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 reachable only on the private network.
- **Sign-in:**

- Advisers and staff sign in through Google Workspace with two-step verification.
 - Clients sign in with a passkey, with Google sign-in, or with a one-time sign-in link sent to their email address.
 - With Google sign-in, two-step verification depends on the client's own Google account, and we recommend turning it on.
 - With an emailed link, access to the client's email inbox is enough to sign in.
 - **Least privilege:** service access is scoped by role and workload identity. An organization policy prevents creating long-lived service-account keys.
 - **U.S. locations:** our Google Cloud organization allows new resources to be created only in U.S. locations.
 - **Audit logging:** actions that create, change or delete data are written to a canonical audit log.
 - **Write-once archive:** audit records are mirrored to a Google Cloud Storage archive whose retention lock is seven years and cannot be shortened.
 - **Monitoring:** cloud-configuration-change alerts, Google Security Command Center findings, dependency scanning, code scanning and PII-egress alerts feed our operational security work.
-

Incident Response and Recordkeeping

Protocol Wealth maintains a written incident response plan. It covers detection, containment, investigation, recovery, post-incident review and customer notification.

Under amended SEC Regulation S-P, we notify affected individuals as soon as practicable, and no later than 30 days after we become aware that their sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. The exception is where a reasonable investigation shows the information has not been, and is not reasonably likely to be, used in a way that would result in substantial harm or inconvenience.

Advisory books and records are kept under the firm's Rule 204-2 program. The rule generally requires five years. Our audit archive is retention-locked for seven.

Vendor and Subprocessor Oversight

Protocol Wealth assesses service providers before engaging them and oversees them periodically under a written oversight program. The public List of Subprocessors names each provider, its role, the data it processes and its security attestations where available. It also notes where diligence on a provider is still in progress.

Representative categories include:

- Cloud infrastructure and internal collaboration.
- AI services.

- Identity verification and sanctions screening.
 - Account aggregation, through Quiltt and its data-provider network.
 - Custodial data delivery, through Nexhelm (with BridgeFT), for accounts at Charles Schwab & Co., Inc.
 - Custody, brokerage, trading and digital-asset infrastructure.
 - CRM, communications and document-signing services.
-

Self-Custodial Digital Assets

Protocol Wealth has built a self-custodial wallet for clients who hold crypto. **It is not offered to clients today.** Its only live use is the owner's test account, where sending from the wallet has been enabled since September 24, 2026.

In this model the client, through a passkey, is the sole root user of the wallet. A provisioning check keeps a wallet from activating while Protocol Wealth is in the root quorum. The firm offers no wallet recovery service today.

Compliance Framework

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

The firm also maintains an ISO/IEC 27001:2022-aligned Information Security Management System, with a Statement of Applicability and a Risk Register. This is an internal control framework and a 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.

Current Limitations

These are not claims of completed controls:

- Customer-managed encryption keys (CMEK) and column-level field encryption are not in place.
- No formal external penetration test has been completed.
- No scheduled access-review cadence is in operation.
- The independent PII egress check does not yet cover every API egress path.
- Our PII scanning does not remove names, and PDF or image attachments in advisor chat are not scanned.

- We have not yet obtained xAI's SOC 2 report for our vendor file.
 - ISO 27001 certification and a firm-level SOC 2 report are not current claims.
-

Verification and Contact

Qualified partners and institutional reviewers can ask for additional diligence materials under appropriate confidentiality terms. These include 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