Security Overview

Aperon, Inc. · Public · October 2026

> Aperon builds software that clinical trial sponsors rely on to keep a complete, auditable record of trial operations. This overview describes how we protect that data: how the platform is built, who can access it, and how we detect, respond to and recover from problems.

About Aperon

Aperon, Inc. is a clinical trial technology company based in Cambridge, Massachusetts. The Aperon Platform captures trial communications and documents as they happen, organizes them into a continuous, auditable record of trial operations, and helps sponsors monitor study activity and get answers backed by cited source records.

Compliance at a glance

Area	Status
SOC 2	Type I audit in progress with an independent CPA firm. The Type II observation period begins November 2026. Controls are monitored continuously in Vanta.
HIPAA	A HIPAA compliance program with approved Compliance, Privacy, Workstation Security and Breach Notification policies. Hosted on HIPAA-eligible Google Cloud services under a BAA.
21 CFR Part 11	The platform is designed to support customers' Part 11 obligations for electronic records: secure audit trails, access controls, record export and tested backups, with a requirements-to-test traceability matrix.
Penetration testing	An independent third-party assessment at least annually. The most recent was in October 2026 and found no critical or high-severity issues.
Policies	15 SOC 2 security policies, plus HIPAA policies, approved by management and reviewed at least annually.

Single-tenant architecture

Every Aperon customer gets a **dedicated, single-tenant environment** in its own Google Cloud project. Each environment has its own:

- application services and service identities;
- PostgreSQL database instance and document storage;
- encryption secrets;
- private network and firewall policy;
- web application firewall policy and logs.

Customers never share a database, and there is no network path between customer environments. Infrastructure is defined as code, so every environment is built the same way and every change is reviewed and recorded.

Infrastructure and network security

- **One way in.** Customer traffic enters only through Google's global load balancer over HTTPS with TLS 1.2 or higher. Plain HTTP is redirected.
- **Web application firewall.** Every customer environment has its own Google Cloud Armor policy. It enforces OWASP Top 10 protections, blocks scanners and exploit paths, and rate-limits sign-in endpoints.
- **DDoS protection.** Google's global edge absorbs volumetric attacks.
- **Private by default.** Only the web application is reachable, and only through the load balancer. The internal API, the database and document storage are not exposed to the internet.
- **Egress allowlist.** Outbound traffic is denied by default. Only a short list of approved destinations is allowed, and anything else is blocked and alerted on.
- **Intrusion detection.** Several layers work together: the WAF, egress denial alerts, Google Security Command Center Premium threat detection across the whole cloud organization, and application-level brute-force detection.
- **Annual reviews.** Firewall rules and network architecture are reviewed against a documented baseline at least annually.

Our *Infrastructure & Network Security Overview* is available on request through the Trust Center.

Data protection

- **In transit:** TLS 1.2+ on every connection, with HSTS. Database connections require TLS.
- **At rest:** AES-256 encryption by Google Cloud for databases, backups, documents and secrets. Sensitive configuration such as SSO client secrets is also encrypted at the application layer with a key specific to each customer.
- **Secrets:** generated automatically for each environment and stored in Google Secret Manager. Secrets are never kept in source code or printed in logs.
- **Data location:** United States by default. Documents are stored redundantly across two US regions.
- **No sensitive data in logs or email:** ingested email bodies are not logged, and notification emails never contain clinical or trial data.

Application security

- **Single sign-on** through OpenID Connect with Google Workspace, Microsoft Entra ID or any OIDC provider. Customers can enforce SSO and require an MFA claim from their identity provider.
- **Strong local credentials.** Passwords are at least 14 characters with complexity and denylist checks. Accounts lock after repeated failures, and brute-force attempts raise an alert.
- **Sessions** end after 2 hours of inactivity and after 12 hours at most, and are revoked immediately when a role changes or an account is disabled.
- **Role-based permissions** (Admin, Manager, Member) that deny by default.
- **Tamper-resistant audit trail.** Database-level protections prevent audit entries from being altered or deleted. Every entry records who acted, when, and the before and after values.
- **Hardened web layer:** Content-Security-Policy, HSTS, frame denial, nosniff and a strict referrer policy on every response.

Access control

- Workforce access uses Google Workspace single sign-on with **MFA required**.
- Production access follows least privilege and is limited to authorized operations personnel with a documented approval.
- Routine production changes are made by automated pipelines with short-lived, keyless credentials. No long-lived cloud keys are issued.
- Access is reviewed at least quarterly and revoked within three days of termination.

Secure development

- Every change goes through a pull request to a protected branch, and required automated checks must pass before merge.
- GitHub CodeQL static analysis and Dependabot dependency scanning run continuously.
- Releases are versioned, documented in release notes, and validated in non-production environments with synthetic data before they reach customers.
- Every deployment keeps an infrastructure plan and a qualification record.

Monitoring, incident response and resilience

- **Centralized logging and alerting** for security events, infrastructure health and uptime. Uptime is checked from multiple regions every five minutes.
- **Seven-year, tamper-resistant archive** of infrastructure audit logs.
- **Incident Response Plan** with defined severities, escalation and root-cause analysis, tested at least annually. Customers are notified without undue delay.
- **Backups:** daily, kept for 30 days, with point-in-time recovery for the previous seven days. Restoration is tested automatically every month for every customer environment.
- **High availability:** databases have a standby in a second zone with automatic failover, and documents are stored across two regions.
- **Status page** on independent infrastructure, showing availability, incidents and planned maintenance.

People and vendors

- Background checks for new employees, and confidentiality agreements and a code of conduct at hire.
- Security awareness training at hire and annually, plus HIPAA training where relevant.
- Managed, encrypted company devices with anti-malware protection.
- Vendors are risk-assessed before onboarding, and critical vendors are reviewed annually.

Contact

Purpose	Contact
Report a vulnerability or security concern	security@aperontrials.com
Privacy and data requests	privacy@aperontrials.com

Purpose	Contact
Customer support	support@aperontrials.com