Elera Health — Security & Compliance Overview

Sep 20, 2026

1. Document control

This is Elera Health's controlled security-review document, version 1.4. It is the architecture and assurance material the public Trust Center refers customers to, and is published there as ELR-SEC-001.

Field	Value
Document	Elera Health Security & Compliance Overview
Document ID	ELR-SEC-001
Version	1.4
Effective date	Sep 20, 2026
Classification	Public
Document owner	Will Tobey, CTO
Review cycle	Every six months, and after any material change to infrastructure or subprocessors
Next scheduled review	Apr 1, 2027
Related documents	Trust Center (getelera.ai/trust), Privacy Policy, Business Associate Agreement, Terms of Service

Scope. This document covers the Elera referral coordination platform. That includes the web application used by Elera staff and clinic users, the background workflow workers, Ellie (Elera's AI care coordinator for messaging and voice), the cloud infrastructure they run on, and the subprocessors they use. Customer-operated systems such as EHRs, fax machines, and clinic workstations are out of scope.

Control status. Items in the Security roadmap (Section 16) carry one of four statuses, the same scale used on the public Trust Center.

Status	Meaning
Operational	Implemented in production today
Strengthening	Implemented, with improvements underway
In progress	Being implemented now
Planned	Committed, not yet started

2. At a glance

Elera Health, Inc. coordinates specialist referrals for medical practices as a HIPAA business associate, from the moment a referral is sent until the patient is seen. Ellie, Elera's AI care coordinator, carries out much of the outreach under the supervision of Elera staff. The answers below are the ones practice security teams ask for first. Every open item appears with its status in the Security roadmap (Section 16).

Question	Answer
Will Elera sign a BAA?	Yes. Elera signs a BAA with every practice before receiving any patient data.
Where is our patients' data stored?	In the United States. Elera's database and file storage are hosted in the US.
Is PHI encrypted?	Yes. TLS 1.2 or 1.3 in transit to the application and storage services, and AES-256 at rest in the database and file storage.
Can we see who accessed our patients' records?	Yes. Every case and patient-list read is logged with the user, time, and outcome. Elera provides an access report for your practice on request.
Is multi-factor authentication available?	We require MFA for all internal users with cross clinic access and offer it optionally to clinics on the platform.
Can our staff sign in with our identity provider (SSO)?	Not yet. SAML and OIDC single sign-on is planned.
How quickly will you tell us about a breach?	Within 72 hours of confirming that an incident affected your patients' data, and never later than the BAA's 60-day limit.
Do subprocessors that receive PHI sign BAAs?	All subprocessors receiving PHI sign BAAs.
Is our data used to train AI models?	No. All AI usage is done through ZDR agreements and BAAs aligned to HIPAA standards.
Do you access our EHR?	Only if your practice opts in, under a portal login you issue. The password stays in the automation vendor's vault and never reaches Elera.
Do you have a SOC 2 report or penetration test?	Not yet. Elera regularly conducts self-driven penetration tests, but has not contracted with an independent tester.
What happens to our data if we leave?	Elera returns or destroys it within 30 days and confirms destruction in writing.

3. How Elera handles your patients' data

Elera receives only what it needs to coordinate a referral, keeps it in one system of record, and shares it with a subprocessor only when a specific task requires it.

What Elera receives [For Referring Physicians]

- Referral packets your practice sends by fax or upload. These include demographics, insurance, reason for referral, diagnosis codes, clinical notes, and any clinical photographs in the packet. Photographs are stored and protected exactly like every other referral document.
- Text messages and calls with patients and families about scheduling.
- Updates from specialist offices: receipts, appointment confirmations, and requests for information.
- Insurance eligibility responses for the patient's plan.

Class	Examples	Where it is stored
Protected health information	Patient names, dates of birth, contact details, insurance identifiers, referral documents and photographs, diagnoses, messages, call recordings, transcripts	Elera's system of record, and only the subprocessors in Section 11
Confidential	User accounts, practice and specialist directories, audit records, operational logs	Elera's system of record and monitoring tools
Public	Marketing site, published policies and agreements	Public website

EHR portal access. If your practice opts in, Elera posts referral updates and documents back to the patient's chart through your EHR's web portal, using browser automation run by CloudCruise. The portal login is stored in CloudCruise's credential vault. Elera's database holds only a reference to it, so the password never reaches Elera and a leak of Elera's data could not be used to sign in. Automated runs are captured in screenshots that Elera keeps in private storage for review. Non-production environments run these tasks in dry-run mode and never write to a real portal.

What Elera receives [For Referral Recipients]

- Elera already has the referral packet in hand, with patient demographics, insurance, clinical history, etc.
- Elera has already corresponded with patient via text messages and calls with patients and families about care coordination
- Insurance eligibility responses for the patient's plan.

Class	Examples	Where it is stored
Protected health information	Patient names, dates of birth, contact details, insurance identifiers, referral documents and photographs, diagnoses, messages, call recordings, transcripts	Elera's system of record, and only the subprocessors in Section 11
Confidential	User accounts, practice and specialist directories, audit records, operational logs	Elera's system of record and monitoring tools
Public	Marketing site, published policies and agreements	Public website

EHR portal access

- Elera accesses your EHR with the most limited possible scope. We read scheduling availability and patient names to match inbound patients to existing patients.
- Elera writes scheduling information and patient information into the EHR.

4. Data flow

Patient data moves along eleven numbered paths. Every internet connection to Elera's application and workers uses HTTPS. Fax, text, and phone legs travel over carrier networks, as they do for any practice. Only path 11, Ellie's calls to specialist offices, carries no patient identifiers.

W#	From and to	What moves	Protection
1	Elera staff to the web application	Patient records needed for coordination	HTTPS (TLS 1.2 or 1.3), individual sign-in, role check on every request. Support sessions are read-only and audited.
2	Practice staff to the web application	Your practice's referrals and patients	HTTPS (TLS 1.2 or 1.3), individual sign-in, access limited to your practice's patients
3	Your fax line and EHR portal, through Sinch and CloudCruise, to Elera's workers	Referral packets in, status notes and documents back to the chart	Fax over the phone network. The EHR login stays in CloudCruise's vault. HTTPS to Elera.
4	Patients and families, through Twilio, to Elera's workers	Scheduling texts and calls	Carrier text and voice to Twilio, HTTPS to Elera
5	Specialist offices, through Sinch and Google, to Elera's workers	Referral packets out, receipts and appointment updates in	Fax and email to the vendors, HTTPS to Elera. Outgoing fax links expire after one hour.
6	Web application and workers to the system of record	All stored PHI and audit records	Server-only credentials. Database roles a browser could reach hold no privileges. AES-256 at rest.
7	Elera to Anthropic and OpenAI	Document text, messages, case details	HTTPS with API keys. No model training. OpenAI response storage off.
8	Workers to Temporal Cloud	Workflow state, potentially including patient data	TLS; each payload encrypted with Elera's own key before it is sent; encrypted at rest by Temporal
9	Elera to Stedi and Google Maps	Name, date of birth, and member ID for eligibility; home address for geocoding	HTTPS with API keys

W#	From and to	What moves	Protection
10	Elera to Langfuse and Sentry	AI inputs and outputs for quality review; application logs, error reports, and traces	HTTPS. Both operate under BAAs. AI content is stripped from traces before they reach Sentry.
11	Ellie to specialist offices	Patient age, reason for referral, insurance plan	Phone call. Never name, date of birth, or contact details.

5. Shared responsibility

Elera secures the platform, its subprocessors, and its workforce's access. Your practice controls which of its staff have access and what it shares.

Area	Elera	Your practice
User accounts	Creates accounts only by invitation, and deactivates any account immediately on request	Requests access only for staff who need it, and tells Elera the same day someone leaves or changes roles
Referral content	Protects everything it receives as PHI	Sends only what the specialist needs for the referral
EHR portal access	Uses the portal login only for the tasks your practice enables, and never handles the password	Issues a dedicated, least-privilege portal account, and revokes it to end access at any time
Suspected compromise	Notifies your practice as described in Section 14	Tells Elera promptly about any suspected compromise of a user account or device
Patient rights requests	Provides records and disclosure history so your practice can respond	Receives and answers patient requests for access, amendment, and an accounting of disclosures
Workstations	Minimizes workstation vulnerability through operational policies and auditing, and uses MFA to prevent compromise.	Keeps staff devices and browsers patched, encrypted, and screen-locked

6. Compliance and governance

Elera's security program is built to the HIPAA Security Rule, owned by a named officer, and self-attested today. HIPAA offers no government certification for products, and Elera has not yet completed an independent audit such as SOC 2.

Accountability. Will Tobey, CTO, is Elera's designated security and privacy official and the owner of this document.

Business associate agreement. Elera signs a BAA with every practice before receiving any patient data. The standard agreement is reviewed and executed electronically, and the signed copy is rendered from the same text the practice read. Its key terms:

- PHI is used only for referral coordination, scheduling, insurance verification, and related administrative services.
- Subcontractors that receive PHI must agree in writing to the same restrictions and safeguards.
- Breaches of unsecured PHI are reported without unreasonable delay and no later than 60 days after discovery. Elera's own commitment is shorter (Section 14).
- Elera supports the practice's obligations for patient access, amendment, and accounting of disclosures.
- On termination, PHI is returned or securely destroyed (Section 15).

Internal assessment. Elera completed its latest quarterly internal code-level assessment of the platform against the HIPAA Security Rule and the SOC 2 Trust Services Criteria for Security, Availability, and Confidentiality. Outstanding items are tracked in the Security roadmap (Section 16).

7. Access control

Every user signs in with an individual account, and every request for patient data is authorized on the server against that user's role and practice before any record is read.

Authentication. Users sign in with email and password. Accounts are created only by invitation, using single-use links that expire after seven days. Every page request checks a signed session token, and every server operation re-validates the user and rejects disabled accounts. Deactivating a user also blocks the account at the authentication provider, so access ends immediately. Every session expires after 24 hours, and ends after an hour without activity: an open screen signs out after a two-minute warning, and a session left on a closed laptop ends at its next use. Sign-in attempts are limited per network address and per account. Single sign-on is on the Security roadmap.

Roles. One authorization library, shared by every server path, enforces these roles. A denied record is indistinguishable from one that does not exist.

Role	Held by	Patient data access
Platform administrator	Elera staff	All patients. Manages users and may start read-only support sessions.
Coordinator	Elera care coordinators	All patients, to coordinate their referrals
Clinic user	Your practice's staff	Only patients referred by or to your practice

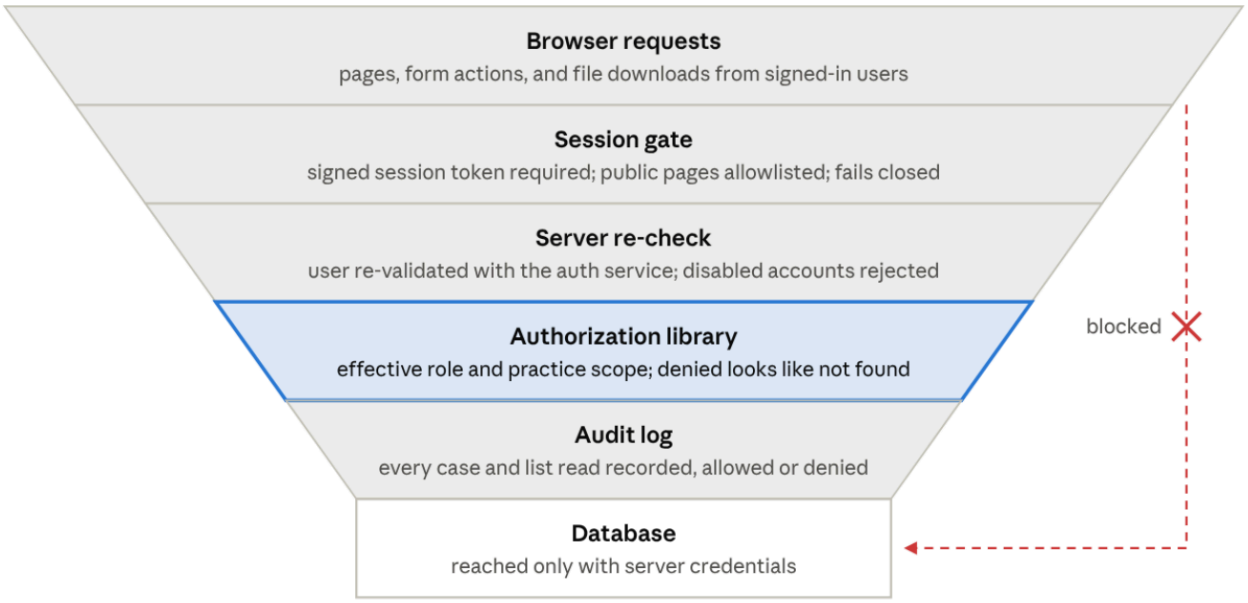
Support sessions. To troubleshoot, a platform administrator can view the product as a specific user sees it. Support sessions are read-only, expire after eight hours, and are bound to the administrator

who started them. The administrator stays the recorded actor in the audit trail, each session's start and end are logged, and a banner stays on screen throughout.

Least privilege. The browser never queries the database directly. All patient data passes through server code that applies the checks above, and the database roles a browser could reach hold no privileges at all. Infrastructure credentials are confined to server-only code.

Every patient-data request narrows through one authorization library

Band width shows narrowing access, not request volume.



Blocked path: database roles a browser could use hold no privileges, revoked and checked on every deploy.

Authorization bottleneck · 5 stages from browser to database

Every request passes the session gate, a server re-check, and a centralized authorization library, and is recorded in the audit log before it reaches patient data. The browser has no route of its own to the database.

8. Infrastructure, data residency, and encryption

Elera's database, application, and workers run on managed cloud platforms in US regions. Elera encrypts PHI in transit on every public connection, and stores it encrypted at rest. Elera operates no physical servers or data centers. Each platform provides physical and environmental safeguards under its own compliance program.

Component	Platform	Region	Purpose
Database, authentication, file storage	Supabase (managed Postgres)	US West (Oregon)	System of record for patients, referrals, documents, and the audit trail

Component	Platform	Region	Purpose
Web application and API	Vercel	US West (Portland)	The product your staff use, and its server-side API
Workflow workers	Fly.io	US West (San Jose)	Background work: fax intake, outreach, AI tasks. At least two machines run at all times.
Workflow orchestration	Temporal Cloud	Managed by Temporal	Durable state for long-running referral workflows

Encryption.

- **In transit.** The web application accepts only TLS 1.2 and TLS 1.3 with forward-secret ciphers, redirects all HTTP to HTTPS, and sets HTTP Strict Transport Security for two years (Vercel). The database's storage and authentication APIs accept only TLS 1.2 and 1.3 (Supabase). Every database connection uses TLS verified against Supabase's certificate, and the database refuses plaintext connections. Worker hosts force HTTPS, and every call to a subprocessor uses its HTTPS API.
- **At rest.** Supabase encrypts all customer data at rest with AES-256 (Supabase). Temporal Cloud encrypts workflow history at rest under its own program, and before any workflow data leaves Elera's systems, Elera encrypts each payload, including error messages, with its own AES-256-GCM key. Temporal Cloud therefore stores workflow data only as ciphertext. Elera platform administrators can read decrypted workflow data in Temporal's console only through an Elera-hosted endpoint that confirms the person is an active platform administrator and records every request in the audit log.
- **Documents.** Users never receive storage links. Files are streamed through authorized requests and marked not to be cached. When the fax provider must fetch an outgoing referral packet, Elera issues a signed link to that single file that expires after one hour.
- **Secrets.** Credentials live in managed secret stores (Doppler, and the encrypted settings of GitHub, Vercel, and Fly.io), never in source code. EHR portal passwords never enter Elera's systems at all (Section 3).

Network boundaries. Only two kinds of endpoint face the internet. The first is the web application, which requires a signed-in session everywhere except public marketing and agreement pages and fails closed if misconfigured. The second is callback endpoints for communications vendors. Sign-in, public forms, and vendor callbacks are rate-limited per network address. **The database accepts no browser-originated queries**, internal services authenticate to one another with shared secrets, and developer endpoints are disabled in production.

9. Audit logging and monitoring

Every case and patient-list read in the product is written to an audit log, whether it was allowed or denied, and the database itself prevents that log from being changed or deleted.

What is recorded. Each audit record captures the time, the actor (a person or a system process), the effective user, any administrator viewing through a support session, a request identifier, the action, the record touched, the decision and its reason, and how many records a list returned. The log also captures:

- Sign-ins, sign-outs, failed sign-ins (with the email stored only as a one-way hash), and password resets
- The start and end of every support session
- Role changes, account deactivation and reactivation, invitations, and practice membership changes

Integrity. Database triggers reject any attempt to update, delete, or truncate audit records, and application roles hold no privileges to alter them. Audit records are kept indefinitely. Separately, every change to a referral is recorded with its actor in an append-only event history, and staff corrections require a stated reason.

Access reports for your practice. On request, Elera provides a report of every recorded access to your practice's patients: who, when, what, and whether it was allowed. Elera platform administrators review activity on a dedicated access-log page.

Operational monitoring. Application logs, error reports, and performance traces are centralized in Sentry, which operates under a BAA. Data is minimized before it leaves the application. Error logs drop database query parameters and request bodies, and traces drop AI prompts and responses. Browser error reports lose URL query strings and free-text messages, and browser session replay, when enabled, masks all text, inputs, and media. Failed production deployments automatically alert the engineering team's channel.

10. AI governance

Elera uses AI to read referral documents, write and classify messages, and run Ellie's outreach. AI at Elera coordinates referrals; it does not diagnose patients or recommend treatment, and Elera's model providers do not train on its data.

Use	Model provider	What the model sees
Reading incoming referral documents	Anthropic	Document text
Writing and classifying messages, summarizing cases	OpenAI	Message threads and case details
Ellie's phone calls to specialist offices	OpenAI and speech models	Patient age, reason for referral, insurance plan. Never name, date of birth, or contact details.

- **Patient communications.** Ellie writes the scheduling texts that patients and families receive, as a care coordinator working on behalf of your practice. Elera staff supervise her work and can review, pause, or take over any case at any time.

- **No training.** OpenAI and Anthropic process Elera's data under commercial API terms that do not allow it to be used for model training.
- **No stored responses.** Every OpenAI request from the web application and workers is sent with response storage turned off. A shared wrapper sets this on each request, and a lint rule blocks code from calling the provider without it.
- **Quality review.** Full AI inputs and outputs are kept for quality review only in Langfuse, under a signed BAA. Traces sent to Sentry have AI content stripped before they leave the application.

11. Subprocessors

Thirteen subprocessors receive PHI to deliver the service, and all have executed BAAs. Each must agree in writing to the same restrictions and safeguards that bind Elera, and Elera gives practices 30 days' notice before adding a new subprocessor that will receive PHI.

Subprocessor	Purpose	Patient data received	BAA
Supabase	Database, authentication, file storage	All patient records and documents	Executed
Vercel	Web application hosting	Patient data in transit through the application	Executed
Fly.io	Workflow worker hosting	Patient data processed by background workers	Executed
Temporal Cloud	Workflow orchestration	Workflow state, including extracted referral details, encrypted with Elera's key before it reaches Temporal	Executed
Anthropic	AI reading of referral documents	Document text, messages, transcripts	Executed
OpenAI	AI messaging, summaries, and coordination	Messages, transcripts, case summaries	Executed
Twilio	Patient texts, staff calls, number checks, call telephony	Message content, call recordings and transcripts, phone numbers	Executed
Sinch	Fax sending and receiving	Referral documents	Executed
CloudCruise	Automated EMR portal tasks	Name, date of birth, referral documents, messages	Executed
Langfuse	AI quality tracing	Full AI inputs and outputs	Executed
Sentry	Logs, error monitoring, and performance traces	Application logs, error reports, performance timings	Executed
Stedi	Insurance eligibility checks	Name, date of birth, insurance member details	Executed

Subprocessor	Purpose	Patient data received	BAA
Google	Address geocoding and lookup, Email	Address geocoding, specialist and patient communication	Executed

Tools that never receive patient data, such as source control, secrets management, team chat, and scheduling, are not listed.

12. Secure development and change management

Every change reaches production through automated gates, and only the merged main branch deploys to production.

- **Checks on every change.** Every pull request runs type checking, linting, formatting, integration tests against a real Postgres database, browser end-to-end tests, and a Semgrep security scan that flags any new finding in the code it adds. The schema check, which applies every migration to an empty database and runs the database-safety guards, must pass before anything can merge; a failure in any other check is fixed in its own follow-up change.
- **Controlled schema changes.** The database schema is defined in code. Migrations are generated from it and never hand-edited, and the production pipeline applies them only after merge.
- **Hardening on every deploy.** Each production deploy revokes all privileges from the database roles a browser could reach, and the deploy fails if any remain.
- **Dependencies.** Installs are lockfile-enforced, automated dependency and security updates run weekly, deployment tooling is pinned, and only allowlisted packages may run install scripts.
- **Environment separation.** Development, preview, staging, and production are separate environments. Test environments use schema-only databases and simulated vendors, test data is generated rather than copied from production, and developer tooling refuses to run against production.
- **Secure coding baseline.** All database access uses parameterized queries, and the application renders no raw HTML. Every response carries HSTS, anti-framing, content-type, referrer, and permissions-policy headers. Every application page also enforces a Content Security Policy: the browser runs only scripts carrying that request's one-time nonce, so injected script cannot execute, and any violation is reported for review.

13. Business continuity and disaster recovery

The platform is built so that losing any single machine loses no work, and the production environment can be rebuilt from version-controlled code.

- **Durable workflows.** Referral work runs as durable workflows on Temporal Cloud. If a worker machine fails mid-task, the workflow resumes on another worker from its last completed step.
- **Redundant compute.** At least two worker machines run at all times, and the web application runs on Vercel's managed serverless platform.

- **Reproducible environments.** The database schema, deployment pipelines, and storage settings are all defined in code, so an environment can be recreated from the repository.
- **Backups and point-in-time recovery.** Supabase continuously archives the production database and keeps 28 days of point-in-time recovery, so the database can be restored to any moment in that window with at most about two minutes of data loss. Point-in-time recovery stays on under Supabase's HIPAA configuration.

Elera's Contingency Plan (ELR-CON-001) covers backups, disaster recovery, and emergency operations. Restores are tested at least once a year; the first test, on September 20, 2026, restored the production database into a separate project in about nine minutes, and every check against production matched.

14. Incident response and breach notification

Elera notifies your practice within 72 hours of confirming that a security incident affected your patients' data, well inside the BAA's 60-day limit for breaches of unsecured PHI.

What the notice contains. What happened and when, which patients and data were involved, what Elera has done to contain it, what your practice may need to do, and a named contact for follow-up. Elera then provides everything your practice needs for its own notifications under 45 CFR 164.410 and supports any patient or regulator inquiries.

How Elera responds.

1. **Detect.** Failed production deployments automatically alert the engineering team's channel, and application errors surface in Sentry. Reports also arrive through the security contact in Section 17.
2. **Contain.** The on-duty engineer limits exposure by revoking credentials, disabling the affected integration, or rolling back the deployment.
3. **Investigate.** The audit trail (Section 9) establishes which records were touched, by whom, and when.
4. **Assess and notify.** Elera performs the four-factor risk assessment under 45 CFR 164.402 and notifies each affected practice.
5. **Review.** Every production incident gets a written review of its cause, the user-visible failure, the mitigation, and the code correction.

15. Data retention, return, and destruction

Elera keeps your patients' records for as long as it serves your practice. When the agreement ends, Elera returns or destroys them within 30 days and confirms destruction in writing.

While services are active, copies outside Elera's system of record are kept to a minimum:

- **Call recordings.** Once a recording is copied into Elera's private storage, the communications vendor's copy is deleted.
- **AI requests.** OpenAI requests are sent with response storage turned off.

- **Vendor document links.** Links issued to the fax provider expire after one hour.
- **Temporary uploads.** Staged upload parts are deleted once the final document is assembled.

At termination, your practice chooses return or destruction. Returned records include referral documents and case history. Audit records are exempt from destruction and are kept to support investigations and HIPAA documentation requirements.

16. Security roadmap

Twenty items are tracked here, each listed once with its status on the scale in Section 1. The list is updated at every review of this document.

Area	Item	Status
Access	Multi-factor authentication for all x-practice users	Operational
Access	Automatic sign-out of idle open screens	Operational
Access	SAML and OIDC single sign-on for practice staff	Planned
Access	Signature or credential verification on every inbound vendor callback	Operational
Access	Request rate limiting on public forms and callback endpoints	Operational
Data protection	TLS required on every database connection	Operational
Data protection	Application-level encryption of workflow payloads	Operational
Data protection	Content Security Policy with per-request script nonces, enforced on application pages	Operational
Data protection	PHI redaction across every operational log field	Strengthening
Data protection	Written retention schedule with automated disposal	Strengthening
Vendors and AI	BAAs with all subprocessors	Operational
Vendors and AI	Zero-data-retention agreements with every model provider	Operational
Development	Secret-push protection	Operational
Development	Automated code scanning	Operational
Governance	Formal HIPAA risk analysis	In progress
Governance	Written incident response and breach notification procedure	Operational

Area	Item	Status
Governance	Documented activity-review cadence and security alert coverage	Operational
Resilience	Contingency plan with point-in-time recovery and a tested restore	Operational
Assurance	Independent penetration test	Planned
Assurance	SOC 2 examination	In progress

17. Contacts and responsible disclosure

Send security questions, evidence requests, and incident reports to security@elera.health.

Need	Contact
Security and privacy official	Will Tobey, CTO
Security questions, evidence requests, suspected incidents	security@elera.health
Product and account support	support@elera.health

Responsible disclosure. Security researchers who find a vulnerability are asked to include steps to reproduce it. They should avoid accessing, modifying, or retaining patient data beyond what is needed to demonstrate the issue, and give Elera reasonable time to remediate before any public disclosure. Elera will not pursue action against good-faith research that follows these guidelines.