Activity Review and Security Alert Coverage

What Elera Health reviews, how often, and who does it, and which security signals raise an alert today. It implements HIPAA information system activity review, log-in monitoring, audit controls, and access management (45 CFR 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.312(b), 164.308(a)(3)–(4)) and SOC 2 CC6.2–CC6.3 and CC7.2.

Field	Value
Document ID	ELR-MON-001
Classification	Public
Owner and approver	Will Tobey, Security Officer
Version	1.0
Effective	September 17, 2026
Review	At least once a year, and after every SEV1 incident
Applies to	Every Elera workforce member, contractor, and system that handles protected health information (PHI)

1. Cadence at a glance

Review	How often	Who	Record
Activity log review	Weekly, every Monday (or the next business day)	Security Officer	Weekly review record (Appendix A)
Access review	Quarterly: January, April, July, October	Security Officer	Quarterly access record (Appendix B)
Departures and role changes	The same business day	Security Officer, or whoever handles the change	Note in the next weekly record
Alerts	As they arrive	Whoever is on duty	Incident record if it is a security incident

Anything that looks like a security incident moves to the Incident Response and Breach Notification Procedure straight away. It does not wait for the next review.

2. Weekly activity log review

Covers the seven days since the last review. Each item is checked and the result written down, even when nothing is found.

Area	Where to look	What to look for
Access to patient data	Admin › Access log (the application's audit log)	Denied decisions; access outside a user's normal practices or hours; unusually large result lists; any activity by a deactivated account (there should be none).
Support sessions	Access log: support-session start and end events	Every session matches a real support request, ended normally, and showed nothing unexpected.
Sign-in activity	Authentication events in the audit log	Clusters of failed sign-ins (emails are hashed, so look for repeats); rate-limited sign-ins and password resets; resets nobody asked for.
Rate limiting	429 responses in Sentry's request logs	Which routes refused traffic and how often. Repeated refusals from one source may be an attack worth blocking.
Application errors	Sentry issues	New high-priority issues, and errors on sign-in, authorization, or file-serving paths.
Browser policy violations	Sentry, Content Security Policy issues	New blocked sources or directives. Ours to fix if it's our code; investigate if it's unexpected.
Production changes	Slack deployment alerts; GitHub main history	Failed deployments, and confirmation that every production change came through the main branch.
Vendor notices	Email from subprocessors	Security advisories or incident notices from Supabase, Vercel, Fly.io, Temporal, Twilio, Sinch, Google, the AI providers, Sentry, Langfuse, or CloudCruise.

3. Quarterly access review

Scope	Steps
Elera application accounts	Export every active user and role from Admin › Users. Confirm each person still needs access at that role. Deactivate anyone who has left or no longer needs it (deactivation blocks sign-in immediately). Keep platform administrators to the minimum.
Practice user accounts	List practice users who have not signed in for 90 days, and disable them after checking with the practice.
Infrastructure and vendor consoles	Review members and roles in Supabase, Vercel, Fly.io, Doppler, GitHub, Temporal Cloud, Sentry, Langfuse, Twilio, Sinch, Google Workspace, the AI provider consoles, and CloudCruise. Remove leavers, reduce excess privilege, and confirm multi-factor authentication.

Scope	Steps
Secrets and integration keys	Confirm every credential in Doppler is still used and held only where needed. Rotate anything held by a departed person or exposed in an incident. Note keys broader than their use requires.
Business associate agreements	Confirm every subprocessor that receives PHI has an executed BAA, matching the list in the Security & Compliance Overview.

Departures do not wait for the quarter: on someone's last day, deactivate their Elera account and remove their console access the same business day.

4. Security alert coverage

The alerts that exist as of the effective date, and the gaps Elera is closing. The Security Officer updates this table whenever an alert is added or changed.

Signal	Alert today	Gap and next step
Failed production deployment (database migrations, workflow worker, staging)	Yes: a GitHub Actions failure alert posts to the engineering team's Slack channel	Web app production deployments run through Vercel's own integration, not this alert. Add them.
Application errors	Yes: Sentry alerts on high-priority issues	Add targeted alerts for sign-in, authorization, and file-serving errors.
Content Security Policy violations	Collected in Sentry as issues; no alert	Alert on a new CSP issue in production.
Failed or rate-limited sign-ins	Recorded in the audit log and request logs; no alert	Alert on a burst of rate-limited sign-ins or 429 responses.
Support (view-as-user) sessions	Audited; no alert	Notify the Security Officer each time a session starts.
Workflow worker and Temporal health	None found in Elera's alerting configuration	Add a health alert for the worker and for stalled workflows.
Vendor incidents	Vendors notify the Security Officer under their BAAs	Keep vendor security contacts current in the quarterly review.

5. Records

- Weekly and quarterly records go in the reviews folder of Elera's Security drive and are kept for six years.
- Each finding that needs action gets an owner and a due date, tracked until closed.
- Missing a review is itself recorded, with the reason and the date it was done.

Appendix A — Weekly review record

Area	Checked (Y/N)	Findings	Action, owner, due
Access to patient data			
Support sessions			
Sign-in activity			
Rate limiting			
Application errors			
Browser policy violations			
Production changes			
Vendor notices			

Week covered: _____ Reviewed by: _____ Date: _____

Appendix B — Quarterly access record

Scope	Accounts reviewed	Removed or changed	Notes
Elera application accounts			
Practice user accounts			
Infrastructure and vendor consoles			
Secrets and integration keys			
Business associate agreements			

Quarter: _____ Reviewed by: _____ Date: _____

Approval

Approved for use at Elera Health. Changes take effect when the Security Officer approves a new version.

Name	Role	Signature	Date
Will Tobey	Security Officer		