Incident Response and Breach Notification Procedure

How Elera Health detects, contains, investigates, and reports security incidents, and how it decides and delivers breach notifications to the practices it serves. It implements HIPAA 45 CFR 164.308(a)(6) and 164.400–414 for a business associate, and SOC 2 CC7.3–CC7.5, and it carries out the commitments in Section 14 of Elera's Security & Compliance Overview.

Field	Value
Document ID	ELR-IRP-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. Commitments

- **Practices hear from us fast.** Elera notifies each affected practice within 72 hours of confirming that a security incident affected its patients' data, and never later than the 60 days after discovery that our Business Associate Agreement (BAA) allows.
- **Every report is answered.** Reports to security@elera.health are acknowledged the same business day.
- **Every decision is written down.** Each incident, including one we conclude was not a breach, has a written record and risk assessment, kept for six years (45 CFR 164.316(b)(2), 164.414).
- **Every production incident gets a review.** A written review of its cause, the user-visible failure, the mitigation, and the code correction.

2. Definitions

Term	Meaning in this procedure
Security incident	An attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system (45 CFR 164.304).

Term	Meaning in this procedure
Breach	Acquisition, access, use, or disclosure of unsecured PHI not permitted by HIPAA that compromises its security or privacy, unless the risk assessment in Step 4 shows a low probability of compromise (45 CFR 164.402).
Unsecured PHI	PHI not encrypted or destroyed to the standard in HHS guidance. Properly encrypted PHI whose key was not exposed is not unsecured.
Discovery	The first day the incident is known to Elera, or would have been known with reasonable diligence, by any workforce member other than the person who caused it (45 CFR 164.410(a)(2)).
Practice	A covered entity that Elera serves under a BAA.

3. Roles

Role	Who	Responsibilities
Security Officer	Will Tobey	Owns this procedure. Declares severity, decides whether an incident is a breach, approves and sends practice notifications, and signs off the review.
Incident Commander	The Security Officer, unless delegated in writing for a given incident	Runs the response, keeps the incident record current, and coordinates engineering, vendors, and practice communication.
Responding engineer	The engineer on duty, or the first engineer to see the alert	Contains the incident, preserves evidence, and investigates.
Every workforce member	Everyone	Reports any suspected incident immediately to security@elera.health or directly to the Security Officer. Does not investigate on their own or delete anything.

If the Security Officer cannot be reached within two hours during a SEV1, the most senior available engineer acts as Incident Commander until they are reached. Breach decisions and practice notifications still wait for the Security Officer, unless the 72-hour commitment would otherwise be missed.

4. Severity

Level	Examples	Response
SEV1	PHI confirmed or likely accessed or disclosed without authorization. A compromised account or credential with access to PHI. PHI sent to the wrong recipient in bulk. A safeguard such as sign-in, authorization, or audit logging failing in production.	Start the response immediately, at any hour. Notify the Security Officer at once.
SEV2	A suspected incident under investigation. A single misdirected fax, text, or email containing PHI. A vendor reporting an incident that may involve Elera data. A security control degraded without known exposure.	Start within one business hour. Notify the Security Officer the same day.
SEV3	Blocked attacks (refused sign-ins, rate-limited requests, scans). Policy deviations without PHI exposure. Vendor security advisories.	Handle in the normal course of work. Summarize in the weekly activity review.

Raise the severity as soon as new facts warrant it. Never lower it without writing down why.

5. Response steps

Step 1 — Detect and report

Incidents reach Elera through these channels:

- **Reports** from practices, patients, staff, or vendors to security@elera.health, or to the Security Officer directly.
- **Sentry** application errors, logs, and performance traces, plus Content Security Policy violation reports from the browser. High-priority issues trigger a Sentry alert.
- **Deployment alerts** a failed production deployment (database migrations, the workflow worker) posts to the engineering team's Slack channel.
- **The audit log** every access to patient data, with the actor, the effective user, the action, the record, and the decision. Authentication events include sign-ins, failed sign-ins (email stored only as a one-way hash), password resets, sign-outs (including automatic sign-out after an hour of inactivity), rate-limited attempts, and support-session starts and ends.
- **Vendor notices** Elera's subprocessors are bound by their BAAs to tell Elera about incidents affecting Elera data.

Whoever spots a possible incident opens an incident record (Appendix A) and notifies the Security Officer. The clock for the 72-hour commitment starts at confirmation of impact, and the BAA's 60-day limit at discovery. Record both times.

Step 2 — Contain

Limit exposure first. Preserve evidence while doing it (Step 3).

Situation	First actions
Compromised Elera user account	Deactivate the user in Admin › Users. This blocks the account at the authentication provider, so access ends immediately. Then review that user's audit trail.
Leaked secret or API key	Rotate it in Doppler, which syncs to Vercel and Fly.io. Revoke the old key at the vendor, then redeploy.
Faulty or malicious deployment	Roll back. Vercel can restore the previous production deployment instantly; the worker can redeploy its previous Fly.io release.
Compromised integration or vendor	Rotate or remove that integration's credential and pause the affected flow. Ask the vendor for its incident details.
PHI sent to the wrong recipient (fax, text, email)	Ask the recipient in writing to destroy it and confirm that they have. Record what was sent, to whom, and their reply.
Lost or stolen staff device	Deactivate and reissue the person's Elera account so every session ends, and rotate any credentials the device held.

Step 3 — Investigate and preserve evidence

- **Which records, by whom, when.** The audit log answers this for every access through the application.
- **What the system did.** Sentry (errors, logs, traces, CSP reports); Langfuse (AI inputs and outputs, for AI-related incidents); Temporal workflow history; the GitHub history of every production change.
- **Preserve.** Export the relevant audit rows, logs, and traces to the incident folder before any retention window can delete them. Never alter or delete original records.
- **Scope.** List each affected practice and, for each, the patients and data elements involved, as far as can be established.

Step 4 — Assess

For every incident that involves PHI, the Security Officer completes the four-factor risk assessment (45 CFR 164.402(2)) in the incident record. An impermissible use or disclosure is presumed to be a breach unless the assessment shows a low probability that the PHI was compromised.

Factor	What to establish
1. The PHI involved	Its nature and extent: the types of identifiers, clinical detail, and how likely it is that patients can be re-identified.
2. Who received or used it	The unauthorized person, and whether they have their own obligation to protect PHI (for example, another covered entity).

Factor	What to establish
3. Whether it was actually acquired or viewed	For example, whether a misdirected fax was opened, or whether logs show the data being read.
4. How far the risk was mitigated	For example, written assurance from the recipient that it was destroyed.

Also record whether a statutory exception applies (45 CFR 164.402(1)): unintentional, good-faith access by a workforce member acting within their authority; an inadvertent disclosure between people authorized to access PHI at the same covered entity or business associate; or a recipient who could not reasonably have retained it. Write the conclusion and its reasons either way.

Step 5 — Notify

Who	When	How and what
Each affected practice	Within 72 hours of confirming that the incident affected its patients' data, and never later than 60 days after discovery	Written notice from the Security Officer to the practice's designated contact covering: what happened and when; which patients and data were involved (each affected individual, to the extent possible, per 45 CFR 164.410(c)(1)); what Elera has done to contain it; what the practice may need to do; and a named contact. Any other information the practice needs for its own patient notices follows as soon as it is known (164.410(c)(2)).
Patients, HHS, and the media	As the practice decides	The practice is the covered entity and makes these notifications. Elera supplies everything it needs and acts on its behalf only if the practice asks in writing.
Law enforcement delay	If an official asks	If law enforcement states that notice would impede a criminal investigation or damage national security: for a written statement, delay for the period it specifies; for an oral one, record it and the official's identity, and delay no more than 30 days unless a written statement follows (45 CFR 164.412).

Our BAA also requires reporting security incidents that are not breaches. Elera reports successful incidents under this procedure. Unsuccessful attempts that never reached PHI (blocked sign-ins, rate-limited requests, scans) happen constantly; Elera records them and gives any practice the details on request. Section 7 tracks making the BAA say so explicitly.

Step 6 — Recover and review

- Restore normal service once containment is verified, and confirm it with the same signals that detected the incident.

- Within ten business days of closure, write the review: timeline, cause, user-visible failure, mitigation, code or process correction, and whether this procedure worked. The Security Officer signs it off.
- Track each correction to completion, and update this procedure or Elera's security documentation when the review calls for it.

6. Records and testing

- **Where.** Incident records, assessments, notices, evidence exports, and reviews go in the incident folder of Elera's Security drive, one subfolder per incident.
- **How long.** Six years from creation or last effective date, whichever is later.
- **Testing.** The Security Officer runs a tabletop exercise at least once a year, using a realistic scenario such as a leaked API key or a misdirected fax, and records what it taught.
- **Training.** Every workforce member reads this procedure at onboarding and when it changes, and knows to report to security@elera.health.

7. Open items

- **BAA wording for unsuccessful attempts.** Elera's standard BAA requires reporting "any Security Incident". Business associate agreements commonly add a clause stating that unsuccessful attempts (pings, port scans, failed sign-ins, blocked requests) occur routinely, are not reported individually, and are described on request. Adding it would make the BAA match Section 5.

Appendix A — Incident record

Field	Entry
Incident ID and title	
Reported by, channel, date and time	
Discovery date and time (starts the 60-day limit)	
Impact confirmed, date and time (starts the 72-hour commitment)	
Severity, and every change with its reason	
Incident Commander and responders	
Systems, practices, patients, and data elements affected	
Containment actions, with times	
Evidence preserved, and where	

Field	Entry
Four-factor assessment and conclusion (breach or not), with reasons	
Notifications sent: to whom, when, and a copy	
Review completed, and corrections tracked	

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		