

Contingency Plan: Backup, Disaster Recovery, and Emergency Operations

How Elera Health backs up patient data, restores service after a failure or data loss, keeps PHI protected while systems are degraded, and tests that all of this works. It implements HIPAA 45 CFR 164.308(a)(7) (data backup, disaster recovery, emergency mode operation, testing and revision, and applications and data criticality analysis) and SOC 2 A1.2, A1.3, and CC7.5, and it carries out Section 13 of Elera's Security & Compliance Overview.

Field	Value
Document ID	ELR-CON-001
Classification	Public
Owner and approver	Will Tobey, Security Officer
Version	1.0
Effective	September 20, 2026
Review	At least once a year, after every restore test, and after every outage that triggers this plan
Applies to	Every Elera production system that stores or processes protected health information (PHI), and every workforce member who operates one

1. Commitments

- **Data loss is bounded.** The production database can be restored to any moment in the last 28 days, losing at most about two minutes of changes.
- **Security stays on.** Sign-in, authorization, encryption, and audit logging are never switched off to restore service faster.
- **Restores are practiced.** A restore is tested at least once a year, and every test and every real recovery is written down.
- **Practices are told.** When an outage will hold up a practice's referral work, the Security Officer tells that practice what is affected and when service is expected back.

2. Recovery targets

The Security Officer approved these targets on September 20, 2026. Restore tests measure against them.

Event	Recovery point (data that can be lost)	Recovery time (until service is back)
Faulty deployment	None	Under one hour, by rolling back
Bad data change or accidental deletion	Up to about two minutes before the chosen restore point	One business day for the affected records
Loss of the production database	Up to about two minutes	One business day
Outage at a hosting provider	None expected; providers keep their own redundancy	As soon as the provider recovers; Elera's part within four hours of it

3. Systems and criticality

Elera's applications and data, ranked by how much referral work stops without them. Sizes are as of September 20, 2026.

System	What it holds	Criticality	How it is recovered
Production database (Supabase Postgres, us-west-2, about 24 GB)	Cases, referrals, patients, messages, tasks, and the audit log: Elera's system of record	Critical	Point-in-time recovery (Section 4)
File storage (Supabase Storage, about 70 GB)	Referral documents and faxes, call recordings, message attachments, portal screenshots	High	Not covered by database backups (Section 4, Section 9)
Web application (Vercel)	No data; stateless	Critical	Redeploy from source, or roll back to the previous deployment
Workflow workers (Fly.io)	No data; stateless	High	Redeploy from source, or the previous release
Workflow orchestration (Temporal Cloud)	Running workflows and 30 days of finished workflow history, encrypted with Elera's key	High	Temporal's own redundancy; durable records live in the database
Secrets (Doppler)	Credentials and keys, including the key that decrypts workflow data	Critical	Doppler's version history
Source code and schema (GitHub)	Application code, database schema and migrations, deployment and infrastructure settings	Critical	Every environment can be rebuilt from the repository

System	What it holds	Criticality	How it is recovered
Communication vendors (Twilio, Sinch, Google)	Calls, texts, faxes, and email in transit	High	Vendor-managed; failed sends are retried from Elera's delivery records

4. Data backup

- **Production database.** Supabase continuously archives the database, at least every two minutes, and keeps 28 days of point-in-time recovery in the same region. Point-in-time recovery is part of Supabase's HIPAA configuration and cannot be switched off. Backups are encrypted at rest.
- **File storage.** Not backed up today. Supabase's database backups contain only the metadata about stored files, and restoring a backup does not bring back files deleted after it. Section 9 tracks closing this gap.
- **Source code, schema, and configuration.** GitHub holds every version. The database schema is declared in code and its migrations rebuild it on an empty database; continuous integration proves this on every pull request.
- **Secrets.** Doppler keeps every version of every secret. The key that encrypts workflow data (TEMPORAL_PAYLOAD_KEY) must never be deleted: workflow history written under it cannot be read without it.
- **Workflow state.** Not backed up separately. Temporal keeps running workflows and 30 days of finished history; cases, referrals, and messages, the records that matter, live in the database.

5. Roles

Role	Who	Responsibilities
Security Officer	Will Tobey	Owns this plan. Declares a disaster, authorizes every restore, decides the restore point, approves practice communication, and signs off the recovery record.
Recovery engineer	The engineer the Security Officer names	Carries out the restore or rollback, verifies the result, and keeps the recovery record current.
Every workforce member	Everyone	Reports outages and suspected data loss to the Security Officer immediately. Never copies PHI into personal or unapproved tools as a workaround.

6. Disaster recovery

The Security Officer declares a disaster when a failure or data loss cannot be fixed by normal operations. If the failure is or may be a security incident, the Incident Response and Breach Notification Procedure (ELR-IRP-001) runs alongside this plan.

Situation	What to do
Faulty deployment	Roll back: Vercel restores the previous production deployment instantly, and the worker redeploys its previous Fly.io release. Fix forward afterwards.
Bad data change or accidental deletion (a bug, a faulty migration, a mistaken operation)	Pick a restore point just before the change. Restore that point into a new, temporary Supabase project, copy the affected records back into production, then delete the temporary project. Prefer this to an in-place restore, which takes the application offline and discards every change made after the restore point.
Production database lost or unusable	Restore in place to the latest good point. The project is offline during the restore, and how long depends on the database's size. Replication subscriptions must be dropped first and recreated afterwards. File storage is not restored and stays as it is.
Outage at Supabase, Vercel, Fly.io, or Temporal Cloud	Follow the provider's status page and support. Temporal workflows pause and resume where they stopped once the service returns. Run Section 7 while the outage lasts.
Secret lost, corrupted, or exposed	Restore the previous value from Doppler's version history, or rotate it under ELR-IRP-001 if exposed. Redeploy so every service picks it up (Fly.io needs its secrets deployed).
Stored files deleted or corrupted	There is no backup to restore from today. Recover what can be re-fetched from its source (a fax vendor, a referring practice), and record what was lost.

After any restore, check before reopening service: the application signs in and loads cases; the newest audit records are close to the restore point; and the workers are processing work again.

7. Emergency operations

While a system is down or degraded:

- **Keep every safeguard on.** Sign-in, authorization, encryption, and audit logging stay enabled. No shortcut that bypasses them is allowed, however urgent.
- **Stop automated outreach that could act on stale or missing data.** Pause Ellie on the affected cases (`pnpm cli ellie runtime disable --case <case id>`).
- **Tell people.** The Security Officer tells the team at once, and tells each practice whose referral work will be held up: what is affected, what Elera is doing, and when service is expected back.
- **Keep PHI where it belongs.** Urgent work continues by phone and fax through Elera's existing accounts. No PHI is copied into personal email, personal devices, or spreadsheets as a stopgap.
- **Catch up deliberately.** Once service returns, work through what was paused before turning Ellie back on, so no family or practice is contacted twice.

8. Testing and records

- **Restore test.** At least once a year, and after any change to how backups work. The Security Officer authorizes each test, because the restored copy holds PHI. Steps and record: Appendix A. The first test, on September 20, 2026, restored production into a new project in 9 minutes 13 seconds, and every check matched.
- **Tabletop.** Once a year, walk through one provider-outage scenario and Section 7 with the team, together with the incident response tabletop.
- **Where.** Test records, recovery records, and reviews go in the contingency folder of Elera's Security drive.
- **How long.** Six years from creation or last effective date, whichever is later.
- **Revision.** Update this plan after every test or real recovery that shows a gap, and at the annual review.

9. Open items

- **File storage backup.** About 70 GB of documents, faxes, and call recordings have no backup independent of Supabase. Options are copying the buckets to a second store under a BAA, or accepting the risk with written reasons.
- **Pausing Ellie everywhere at once.** Today Ellie is paused case by case. A single switch would make Section 7 faster in a wide outage.
- **Restarting workflows after losing Temporal.** Confirm, in a tabletop or the first restore test, that every long-running workflow can be restarted from database state.
- **Rotating the workflow encryption key.** Elera holds one key today. Rotating it needs support for reading data under the previous key first.

Appendix A — Restore test record

Restore into a new, temporary Supabase project in Elera's HIPAA organization. Never connect the application, the workers, or any vendor integration to the copy, so it cannot contact anyone. The copy has its own database password; query it read-only through the Supabase command-line login instead of handling that password. Delete it the same day.

Field	Entry
Authorized by, date	
Restore point chosen (date and time, UTC)	
Restore started, and copy ready (times); elapsed time	
Row counts in the copy versus production as of the restore point (cases, referrals, patients, messages, audit log)	

Field	Entry
Newest audit record in the copy, and its distance from the restore point	
Spot check of known records	
Temporary project deleted (time, by whom)	
Problems found, and changes to this plan	

Appendix B — Recovery record

Field	Entry
Event and date	
Declared by, and time	
Systems affected	
Restore point and method (rollback, copy-back, in-place restore)	
Service restored (time); data lost, if any	
Practices told (who, when)	
Review 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		