EATAL

Emergency Access Trust & Accountability Engineering Layer

Governance for OpenEMR break-glass access – external, non-blocking, always on.

Afraa Haque - Anthony Duong - Nanditha Harish Bhat
Omar Salameh - Reem Mohsen - Prathamesh Upadhye

The Problem

Every day, there are 10,000 emergency-access incidents recorded that a Compliance Officer has to go through, but can only look at 50.

There are no tools for locating instances of Misuse related to the use of these break-glass overrides.

Why It's Broken

- Break-glass overrides bypass all standard access controls.

- The audit logs in OpenEMR are flat (i.e., very basic) therefore; They lack risk priority and a clinical context.

- Compliance Officers "fall back" to doing random sample reviews.

- In HIPAA §164.312(b), it requires demonstration of oversight; sampling won't suffice.
HIPAA Security Rule §164.312(b), Audit Controls Standard

Why It Matters

- 70%+ of healthcare data breaches are due to insiders.
Verizon DBIR, 2024

- 76% of OCR enforcement actions cited a missing risk analysis.
HIPAA Journal, 2025

- The misuse of insider data can occur for months without any way of knowing this is happening.

- Depending on the violation tier will be assessed up to $2M per HIPAA violation.

Solution Overview

Designed to cut manual review by over 50% through customized top-N per institution.

Ingest — Reads OpenEMR audit logs. Does not write any data.

Score — Every event will have an associated risk score and written rationale of that score.

Rank — Event flagged as top-N rises to review queue.

Alert — Drifting is identified early before it becomes a recognized trend.

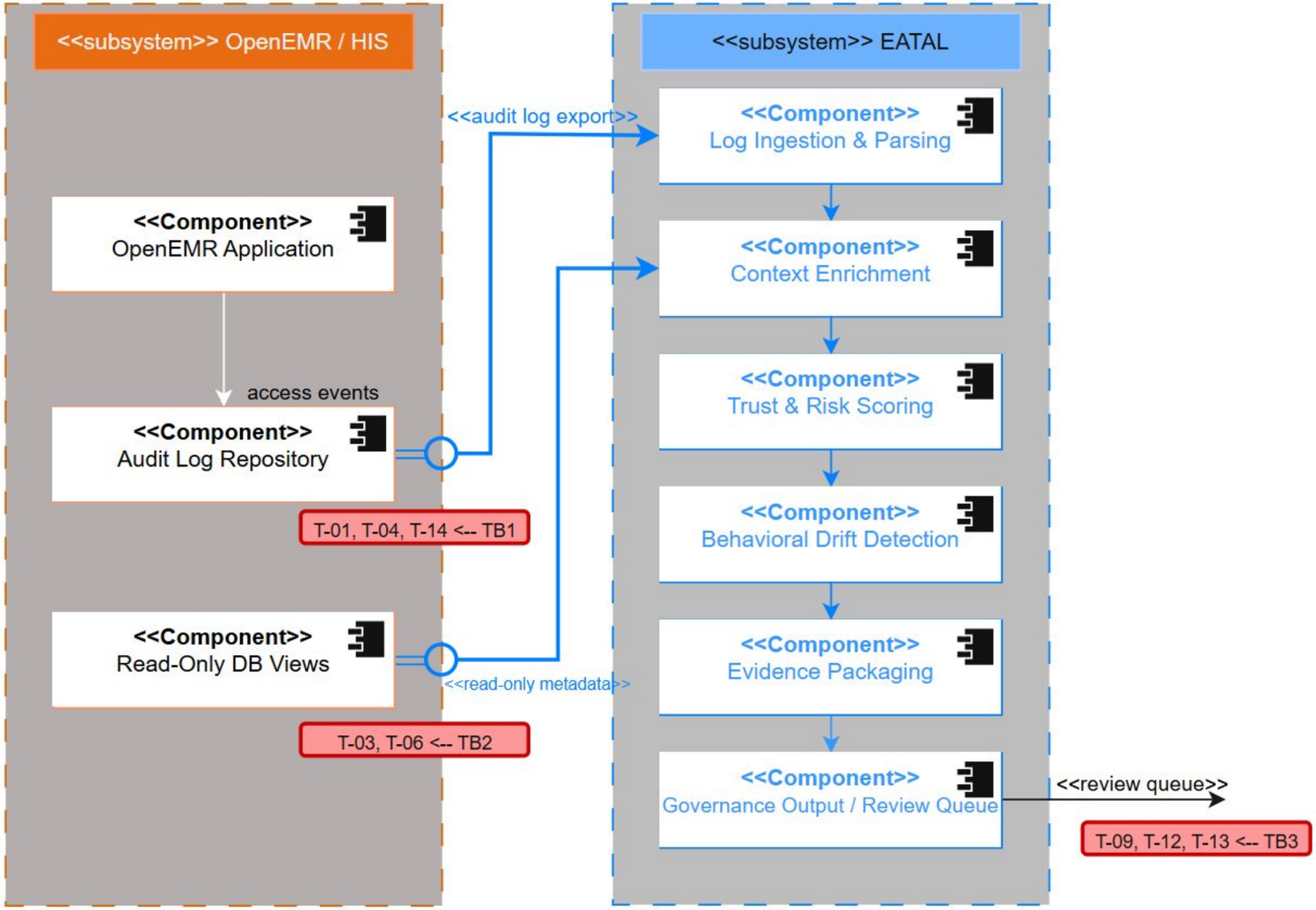
System Architecture

DESIGN TARGETS (per canvas success criteria)

≥50% reduction in manual audit-review effort

<5 min to generate a HIPAA evidence package

0 ms added to clinical access latency



Two subsystems, one boundary. Each interface is read-only and tagged to specific threats.

Threat Analysis

Without EATAL

- Misuse is hard to find
- Logs altered before review
- Break-glass becomes routine
- 10,000 events, no priority

With EATAL

- Scoring done for all overrides.
- Tampering caught at ingest
- Drift alerts fire early
- Top-N flagged for review

What Makes EATAL Different

Zero-touch

OpenEMR does not get modified.
No downtime.
No migration.

Non-blocking

If EATAL were to go down, clinical care will continue.

Context-aware

Not just who accessed it, but if they should have.

Defensible

Every score has a written reason why.
Audit-ready.

Compliance Officers

Top-N review queue,
not 10,000-event sampling

Security Ops

Alerts will be sent prior to abuse of system, not after.

Hospital Leadership

Proactive HIPAA evidence,
not reactive scrambles

Regulators & Auditors

Audit packages assembled in minutes.

— DEMO

EATAL in Action

Conclusion

- Break-glass becomes observable
- Evidence of misuse gets shown earlier
- HIPAA evidence can be produced within minutes
- Patient safety is never compromised

Trust Score: How It Works

Each break-glass occurrence generates a composite score based upon the combination of five weighted signal sets.

Role-shift & Identity

Was this user scheduled to work on this date? Off-schedule access raises risk.

Encounter & Clinical Ctx

Was there a same-day encounter documented for this patient? No same-day encounter = higher scrutiny.

Temporal & Shift

Did the access occur during peak clinical hours (07:00–19:59)? Off-peak access raises risk.

Peer Comparison

How does the user's override rate compare to their peers in these departments? Outlier override volume matters.

PriorEnc Window

Did the user and the patient have a prior encounter within the last 10 days? The lack of any prior encounter increases risk.

Output: trust score 0–100 + per-signal breakdown

Demo example: doctor2 = 15/100 lower score = needs review

WRITTEN RATIONALE – every score is explainable

All scoring has an individual explanation broken down by signal rather than just flagging them as a blackbox. Here is an example of a scoring rationale from the/queue/json endpoint:

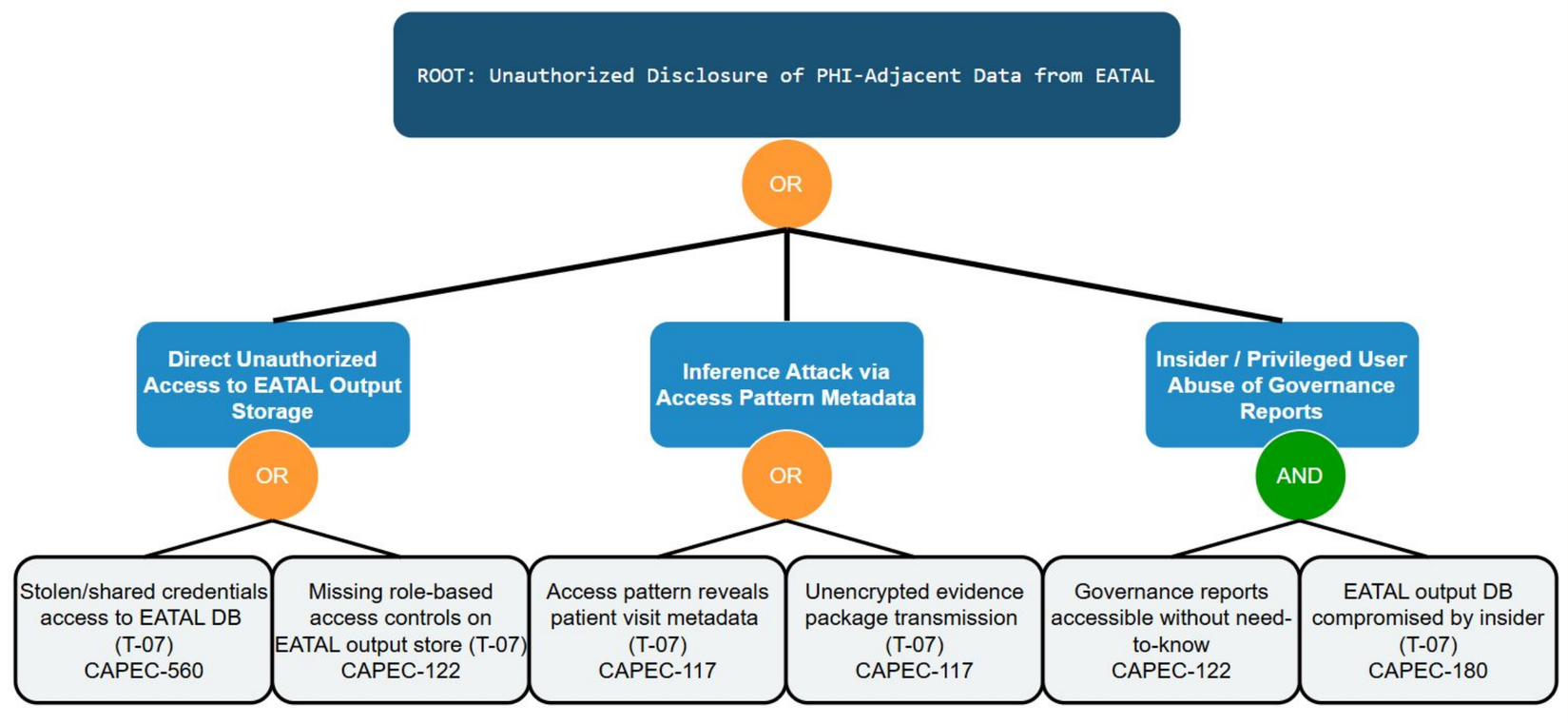
```
"Role-shift: 0.0, Encounter: 20.0, Temporal: 70, Peer: 50.0, PriorEncWindow: 0.0"
```

Each item in the review queue carries this breakdown plus a Decision-support only advisory.

Bayesian model: ~72% posterior probability that insider misuse goes undetected without contextual scoring.
STRIDE threat registry: 14 threats (T-01 through T-14).

Privacy Attack Tree

Full threat decomposition – each leaf maps to a STRIDE threat.



Mitigations Built In

RBAC on EATAL outputs · Encryption at rest and in transit · Pseudonymized patient IDs · Minimum-necessary metadata only · Audit logging on EATAL itself