GEORGE MASON UNIVERSITY

TrustPulse

A Human-Review Workflow for OpenEMR Audit Evidence

Group #1

Ali Hakami | Mansi Patel | Mustapha Badaoui
Nawaf Hakami | Sagar Bhandari | Sidi A. Brahim

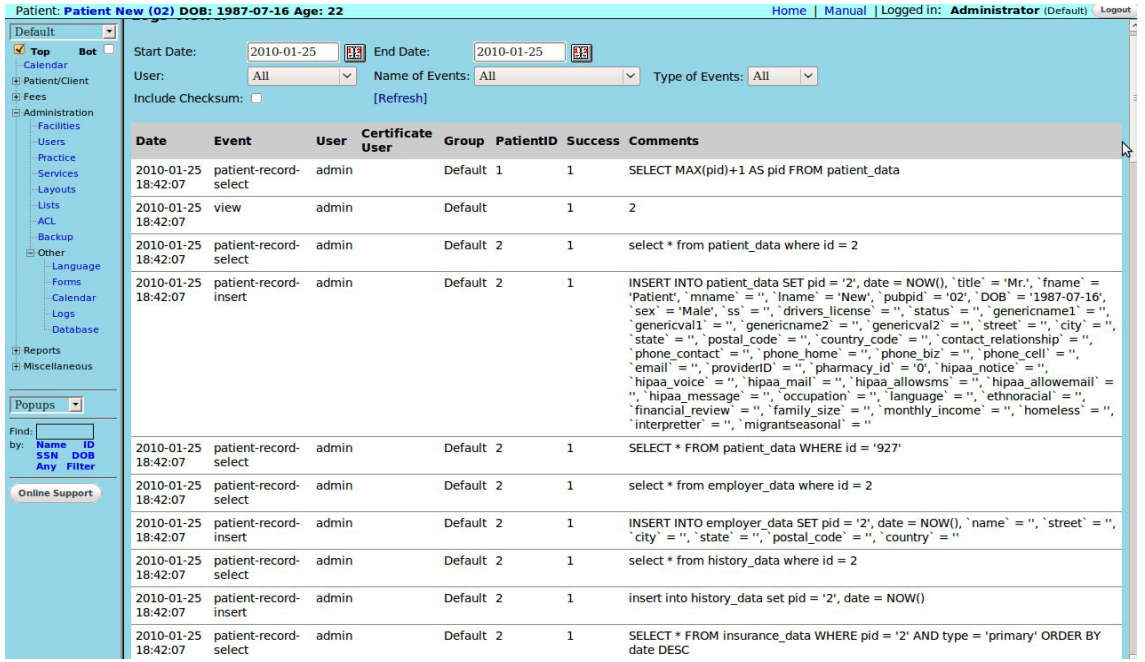
CYSE Systems Engineering Seminar
Dr. Alexandre B Barreto

Agenda

Intro · Problem · Risk Chain · Solution · Design Fit · Boundary · Threats · Governance · Demo · Conclusion

Audit Logs Are Not a Review Workflow

Raw OpenEMR Audit Logs



The gap is not logging. The gap is repeatable, documented review.

GEORGE MASON UNIVERSITY

The Risk Chain Behind Manual Review

RISK CHAIN

1. Incomplete / Noisy Logs
2. Manual Review Overload
3. Missed Access Patterns
4. Weak Audit Trail
5. False Assurance

Risk Propagates

OPERATIONAL IMPACT

Delayed Privacy Review
Reviews delayed and backlogged

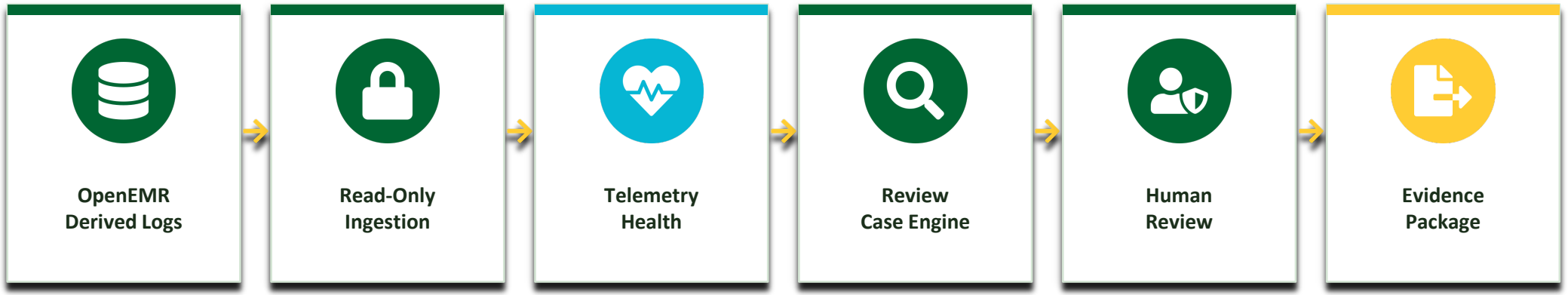
Inconsistent Review Decisions
Decisions vary across reviewers

Compliance Exposure
Review evidence becomes weaker

Loss of Patient Trust
Privacy Concerns reduce confidence

GEORGE MASON UNIVERSITY

TrustPulse: Turning Logs Into Evidence



Not **a SIEM replacement.** Not **an automatic HIPAA violation detector.**
A human-review workflow for OpenEMR audit evidence.

Read-only | Non-blocking | External | Metadata-focused | Explainable Review

GEORGE MASON UNIVERSITY

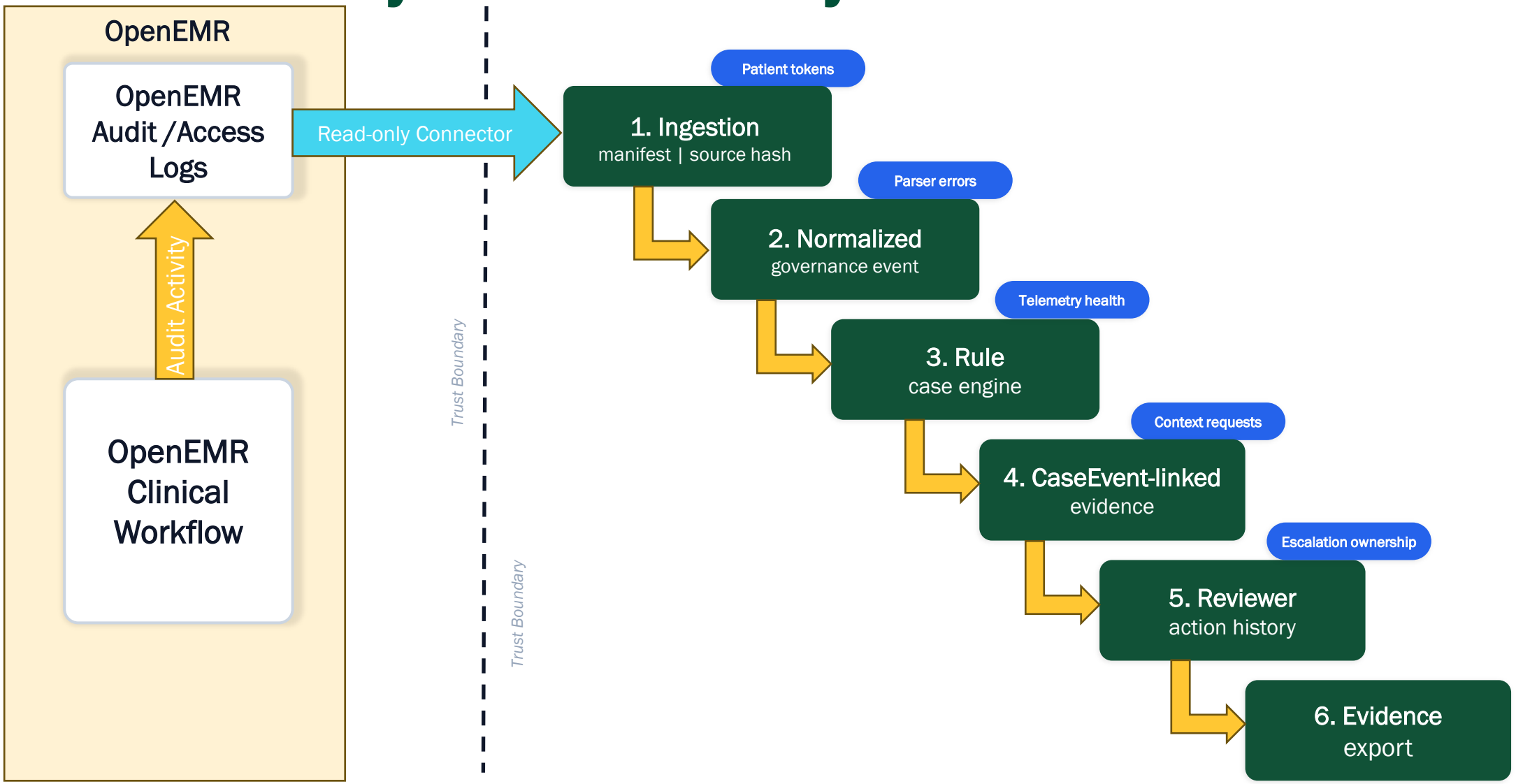
Why This Design Fits Healthcare

Architecture guided by realism, fit, and compliance

Technical Realism	Operational Fit	Healthcare Constraint
Uses existing OpenEMR audit logs	No clinician workflow disruption	Clinical availability preserved
SELECT-only connector	Metadata-focused review	Patient IDs tokenized
Rule-based explainability	Compliance officer remains in control	Human judgment preserved
Separate governance database	Lightweight for small clinics	No OpenEMR modification

External governance layer beside OpenEMR

System Boundary & Evidence Flow

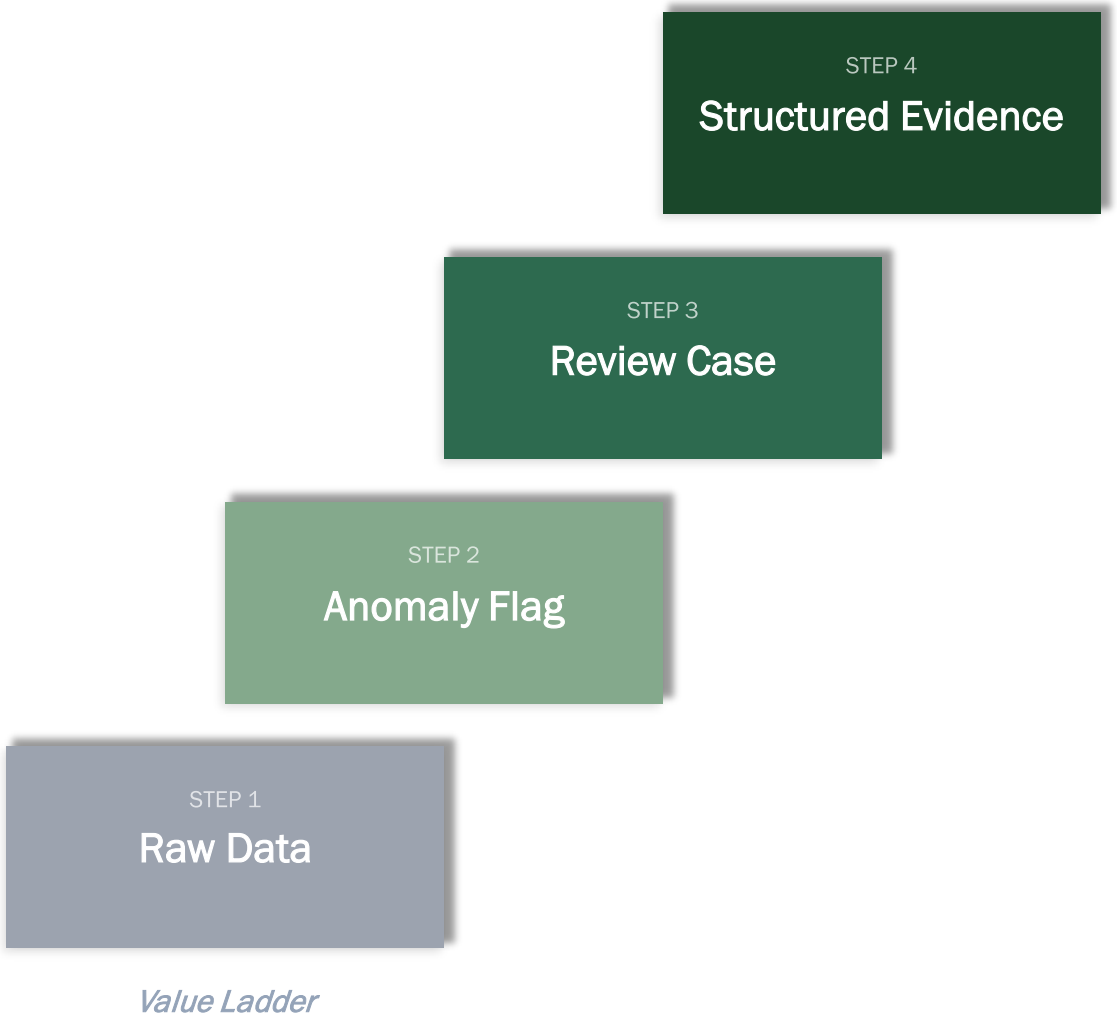


Threat Surface & Trust Controls

THREAT DOMAIN	ATTACK SURFACE	POTENTIAL HARM	TRUSTPULSE CONTROL
01 Source Telemetry	**OpenEMR audit feed:** logs may be incomplete, suppressed, or altered	*Missing or incomplete review → false assurance of coverage*	• Telemetry health checks • Parser error tracking • Ingestion manifests • Source and normalized batch hashes
02 Review Logic	**Thresholds, rules, and Configuration:** a privileged user may suppress cases	*Suppressed or noisy cases → weak review coverage*	• Explainable rule engine • Exact case-event linkage • Baseline/Policy based labeling • Rule limitations when context unavailable
03 Reviewer Workflow	**Dashboard account and disposition actions:** compromised reviewer	*False closure or unauthorized export → weak evidence trail*	• Escalation ownership • Reason-coded actions • Review Action History • Context requests
04 Evidence Export	**Report generation and Interpretation:** Output may be overclaimed	*Overclaiming compliance or exposing sensitive context → regulatory risk*	• Patient ID tokenization • Telemetry health control • Human-review disclaimer • Limitations section

GEORGE MASON UNIVERSITY

Governance Value



Auditor

Exportable, verifiable evidence trails linking raw events to human dispositions.

IT / Security

Clear pathways for authentication and account review.

Clinic Leadership

High-level governance visibility and organizational accountability.

Compliance / Privacy Officer

Faster review queues and documented, auditable decisions.

GEORGE MASON UNIVERSITY

Demo Use Cases

High-Volume Billing Access

Actor: David Ross / Billing

⚠ **Trigger:** Many patient records accessed rapidly.

↓

Request billing justification

↓

Supervisor response

↓

Resolve

↓

Export evidence

Physician After-Hours Access

Actor: Dr. Nguyen / Physician

⚠ **Trigger:** After-hours patient record access.

↓

Request clinical context

↓

Escalate to Privacy Officer

Authentication Review

Actor: Susan Hayes / Admin

⚠ **Trigger:** Repeated failed logins.

↓

Authentication review

↓

Request account confirmation

(Not a patient-access review)

GEORGE MASON UNIVERSITY

Summary & Conclusion

Non-Disruptive Governance

- Operates entirely outside the OpenEMR trust boundary via a read-only connection, ensuring zero impact on clinical availability.

Actionable Oversight

- Eliminates manual log fatigue by translating raw telemetry into prioritized, rule-based review cases.

Traceable Accountability

- Mandates a human-in-the-loop workflow that generates secure, compliance-ready evidence packages.

Technically Realistic

- Delivers a lightweight, feasible governance solution tailored for the operational and privacy constraints of healthcare organizations.

GEORGE MASON UNIVERSITY

Thank you!!

Questions?