Line 3: Zero-Trust, Consent-Aware Governance for Secure HIE

Secure health information exchange governance framework for identity, consent, access control, and audit

Xinyang Li | July 2026

Aligned HITC platform direction: HITC-SecureExchange platform direction

Authorship, Timeline, and Institutional Context

Xinyang Li is presented as the methodology author and technical originator of the framework described in this file. The framework is not presented as a Zymo Research project and is not presented as completed employee work for HITC. It is an independently developed methodological contribution intended for future implementation, validation, and extension through HITC's health informatics research platform environment.

Development period: 2024 through mid-2026. The stated development activities include independent research, literature review, methodological design, and formal specification using health informatics standards and computational methods. The evidentiary record remains under development and should be supported by signed methodology statements, dated drafts, technical design records, draft manuscripts, and research notes before filing as completed Criterion v evidence.

Original Contribution Statement

This framework addresses governance gaps in cross-institutional health information exchange: identity, contextual authorization, structured consent, auditability, and privacy-preserving research access. It specifies a four-layer decision workflow with two privacy-enhancing extensions.

Technical Methodology Brief

- Identity and Authentication: OIDC with clinical role claims, purpose-of-use claim, emergency break-glass protocol, and NIST 800-63 IAL/AAL tiers.
- ABAC Engine: four-domain attribute model covering subject, resource, context, and policy; deny-by-default policy evaluation; XACML 3.0 rule sets with FHIR Policy representation.
- Consent Enforcement: FHIR Consent R4 resources with resource-level granularity, purpose-of-use scoping, and signed revocation propagation targeted within 60 seconds.
- Audit and Provenance: Merkle-tree hash-chained AuditEvent records, cross-institutional linkage using shared transaction IDs, partner organization hash references, and real-time anomaly detection.
- Federated Query Extension: multi-site research queries with cell suppression (minimum n=10) so individual-level data does not leave source organizations.
- Differential Privacy Extension: epsilon-calibrated release mechanism and privacy budget tracking.

Original vs. Existing

Original concepts:

- Cross-institutional audit hash chain that includes partner organization Merkle roots in each organization's audit record.
- Integration of identity, ABAC, consent, and audit into a unified governance decision workflow.
- Resource-level FHIR Consent enforcement with structured revocation propagation.

Existing technology: OAuth 2.0, OIDC, SMART-on-FHIR, XACML 3.0, FHIR Consent R4, differential privacy, Merkle trees, NIST SP 800-63, STRIDE, and OWASP API Security Top 10.

Architecture and Workflow

```
DATA ACCESS REQUEST: clinician / app / researcher with OIDC token
|
L1 IDENTITY: OIDC -> role claims -> purpose-of-use -> break-glass -> NIST assurance
|
L2 ABAC ENGINE: subject + resource + context + policy -> deny-by-default -> permit/deny
|
L3 CONSENT: FHIR Consent R4 -> resource directive -> revocation check
|
L4 AUDIT: AuditEvent -> Merkle hash chain -> cross-org linkage -> anomaly detection
|
ACCESS GRANTED OR DENIED: all decisions audited with provenance context
```

Validation and Benchmark Targets

The ABAC policy decision point should be benchmarked using synthetic policy sets and policy evaluation engines. Consent propagation is modeled from distributed-system behavior. Audit tamper detection is validated through hash-chain and Merkle-tree simulation. Security architecture should be assessed through STRIDE and OWASP API methods.

Important caveat: These metrics are concept-of-concept, simulation-based, or literature-benchmark targets. They do not claim completed production deployment outcomes.

Metric	Target / Projected	Basis	Comparison Benchmark
PDP latency	<20 ms median	XACML engine benchmark; 10,000 events	Conventional RBAC/HIE policy checks
Consent propagation	<60 sec across 45 nodes	Distributed systems model; signed broadcast	Manual consent-update workflows
Audit tamper detection	100% detectable modifications	SHA-256 hash chain; Merkle simulation	Siloed audit logs
Security threats mitigated	6/6 STRIDE categories; 0 critical gaps	STRIDE and OWASP API assessment	Baseline HIE security review

Prospective Validation and Adoption Path

The following prospective validation sites are part of the future research and evidence-development pathway. No completed external deployment is claimed in this standalone split file.

- Regional HIE Security/Compliance Team: prospective site for ABAC engine and audit trail validation. Planned scope: policy accuracy and latency benchmarked against existing RBAC system. Status: initial discussion.
- Academic Medical Center IT/Compliance: prospective site for FHIR Consent resource deployment and consent evaluation workflow testing. Status: research proposal in development.
- Multi-Institutional Research Data Network: prospective site for federated query and differential privacy extension validation. Status: network identified; no engagement yet.

Expert Assessment Plan

Planned expert profile: health information privacy and security researcher or professor with expertise in data governance, HIPAA compliance, and access-control frameworks. Proposed scope: assess the four-layer governance architecture, structured consent enforcement, and cross-institutional audit trail design.

Scholarly and Standards Corroboration

- OAuth 2.0 (RFC 6749) and OpenID Connect: identity protocol foundation.
- SMART-on-FHIR Granular Access: FHIR-specific OAuth scope specification.
- XACML 3.0 (OASIS, 2013): ABAC policy language.
- NIST SP 800-63-3 (2017): digital identity assurance levels.
- FHIR Consent R4: structured patient consent representation.
- HIPAA Privacy Rule and Security Rule: regulatory framework for PHI access and audit.
- Differential Privacy (Dwork et al., 2006), Merkle Tree (Merkle, 1980), STRIDE, and OWASP API Security Top 10.

Academic Field Contribution Argument

- Generality of method: the framework is specified as a transferable methodology, not as an implementation tied to one platform or employer.
- Standards-based formalism: the contribution is expressed using recognized health informatics and security standards.
- Prior-art gap identification: the framework identifies a specific gap in current practice and proposes an incremental method-level contribution.
- Future validation path: the applicant plans peer-reviewed manuscript submission and structured validation studies through HITC's research setting.

Source note: This standalone file was split and reorganized from Li_Xinyang_Original_Contributions_Exhibit_v2.pdf. It preserves the cautious evidentiary status of the source document.