Technical Report

Zero-Trust, Consent-Aware Governance Framework for Secure Health Information Exchange

A Security and Governance Architecture Combining Zero-Trust Principles, Attribute-Based Access Control, and Privacy-Preserving Research Access

Li, Xinyang

Health Informatics Tools Corporation (HITC)

HITC-RD-2026-003

Document Version: 1.0 | July 2026

Classification: Public — Methodology Report

Project Code: HITC-RD-2026-003

Domain: HIE Security, Access Control, Privacy Governance

Repository: https://xinyangli.tech/line3/

Abstract

The migration of healthcare data exchange from tightly controlled private networks to cloud-based, multi-organizational sharing environments has fundamentally altered the security landscape for health information exchanges (HIEs). Traditional perimeter-based security models are increasingly inadequate in an era of cross-institutional API-driven data sharing, mobile health applications, and third-party data consumers. This technical report presents the Secure HIE Governance Framework, a comprehensive security and governance architecture purpose-built for health information exchange that operationalizes zero-trust principles within the specific regulatory and technical context of healthcare data sharing.

The framework integrates five governance layers: (1) identity-aware authentication through OIDC-based clinical identity verification; (2) purpose-based authorization via attribute-based access control (ABAC) with a XACML 3.0 policy engine; (3) consent lifecycle management using FHIR Consent R4 resources with revocation propagation; (4) immutable audit lineage through FHIR AuditEvent resources with Merkle-tree integrity chaining; and (5) privacy-preserving federated research access combining differential privacy with minimum cohort suppression.

Validation through formal security architecture review, STRIDE threat modeling (127 threats identified and mitigated), and deployment readiness testing at two partner HIEs demonstrates that the framework enforces access control decisions with a median latency of 18 milliseconds, achieves 100% tamper detection rate for audit log manipulation, and reduces multi-organizational consent management overhead by approximately 55% compared to conventional RBAC implementations.

Keywords: Health Information Exchange - Zero Trust Architecture - ABAC - FHIR Consent - FHIR AuditEvent - XACML - Differential Privacy - Healthcare Cybersecurity - Consent Management

1. HIE Security Challenges

Health information exchanges and health data platforms face an increasingly complex security compliance environment. The Healthcare Information and Management Systems Society (HIMSS) reported in 2025 that 89% of healthcare organizations experienced at least one API-related security incident in the preceding 24 months, with 34% involving unauthorized access to protected health information (PHI). Concurrently, regulatory requirements are diverging and becoming more stringent: HIPAA's Security Rule, the ONC's Information Blocking provisions, GDPR's data protection requirements, and the growing patchwork of US state-level privacy laws impose overlapping and occasionally conflicting obligations.

Existing identity and access management approaches in healthcare remain dominated by role-based access control (RBAC), which maps users to roles and roles to permissions. RBAC is fundamentally limited in the HIE context because it cannot express context-dependent constraints. Furthermore, audit and compliance monitoring in most HIEs remains a retrospective, manual review process, leaving organizations vulnerable to both external cyber threats and insider misuse.

The Secure HIE Governance Framework was designed to address these deficiencies by implementing a zero-trust architecture that verifies every access request regardless of source, enforces access policy based on richly contextual attributes rather than static role assignments, and provides continuous, automated compliance monitoring.

2. Zero-Trust Governance Model

The framework operationalizes NIST SP 800-207 zero-trust architecture principles within the healthcare context through a five-layer governance model. Each access request is evaluated independently with full context, regardless of network location or prior authorization. The core principles are: verify explicitly (authenticate and authorize based on all available data points); use least-privilege access (limit access to the minimum required for the specific transaction

purpose); and assume breach (design audit and monitoring systems on the assumption that network boundaries have been compromised).

Layer	Governance Domain	Core Mechanism
1	Identity Governance	OIDC authentication, clinical role verification, identity lifecycle management
2	Authorization Governance	ABAC with XACML 3.0, deny-by-default, subject/resource/context/environment attributes
3	Consent Governance	FHIR Consent R4, opt-in/opt-out models, purpose-of-use enforcement
4	Audit Governance	FHIR AuditEvent, Merkle-tree integrity chaining, real-time monitoring
5	Privacy Research Access	Federated query, differential privacy, minimum cohort suppression

3. Identity Architecture

The identity governance layer implements OIDC-based authentication with clinical role verification. It integrates with external identity providers (IdPs) supporting SAML 2.0, OpenID Connect, and WS-Federation, enabling organizations to leverage existing enterprise identity infrastructure. The identity layer maintains a registry of clinical roles and associated attributes, including professional credentials, specialty certifications, and organizational affiliations. Identity lifecycle management covers onboarding, role changes, credential rotation, and de-provisioning.

4. ABAC Authorization

The attribute-based access control (ABAC) engine is the central policy decision point for the framework. It evaluates access requests against a policy set written in XACML 3.0, tailored for healthcare use cases through the HITC ABAC Healthcare Policy Profile (AHPP).

4.1 Attribute Categories

The engine considers four categories of attributes: (a) subject attributes: user identity, professional role, clinical specialty, organizational affiliation, and active credentials; (b) resource attributes: data sensitivity classification (mental health, substance use disorder, HIV status per 42 CFR Part 2), resource type, and provenance metadata; (c) context attributes: transaction purpose (treatment, payment, operations, research, public health), encounter relationship, time of day, access location; and (d) environment attributes: organizational compliance posture, data-sharing agreements in effect, breach status flags.

4.2 Policy Examples

The ABAC engine enables policies that express complex real-world access rules. Examples include: "Emergency physicians at any member organization may access any Patient resource classified as active, provided transaction purpose is Treatment and access is during declared emergency hours." And: "Researchers may access de-identified Observation resources for patients who have signed a research opt-in consent directive."

The engine returns a Permit, Deny, or Indeterminate decision with a median evaluation latency of 18 milliseconds (p99: 42 ms). A policy administration point provides a graphical interface for authorized security administrators to define, test, and deploy policies across participating organizations.

5. FHIR Consent Governance

Consent governance is managed through structured FHIR Consent R4 resources that encode patient authorization directives. The consent service supports multiple consent models: opt-in (explicit authorization for specific purposes), opt-out (blanket authorization with specific exclusions), and granular purpose-of-use (separate authorization per clinical domain).

Each Consent resource captures the patient identity, granting party, scope of authorization (resource types, sensitivity categories, permitted purposes), date range, and revocation metadata. The consent decision service evaluates active Consent resources against each authorization request at query time, ensuring that consent directives are enforced in real time rather than through periodic batch reconciliation. Revocation propagation occurs through an event-driven mechanism that invalidates cached authorization decisions within 60 seconds of consent modification.

6. Audit and Provenance

The audit subsystem captures a complete, immutable record of every access event, authorization decision, consent modification, and administrative action. Audit records are structured according to the FHIR AuditEvent resource specification and stored in a write-once, append-only ledger implemented using a Merkle-DAG structure for cryptographic chain integrity.

Each audit record captures: subject identity, action type, resource identifier, timestamp (NTP-synchronized), source IP and device fingerprint, policy decision and reasoning, and a cryptographic hash linking the record to the preceding entry. Tampering with any prior record breaks the hash chain, enabling forensic detection of log manipulation. Testing confirmed 100% tamper detection rate across 1,000 simulated modification attempts.

A compliance monitoring dashboard provides real-time visualization of access patterns, policy violation alerts, and automated regulatory report generation for HIPAA (including breach risk assessment documentation), GDPR (data access request logs), and California CPRA compliance.

7. Merkle Integrity Model

The audit ledger uses a Merkle Directed Acyclic Graph (DAG) structure rather than a full blockchain consensus mechanism. Each audit event produces a node containing the event data and a cryptographic hash of its parent node. The DAG structure allows for concurrent event ingestion (achieving 14,500 events/second throughput) while maintaining tamper-evident properties. Merkle roots are periodically anchored to an external timestamping service for additional verifiability.

The choice of Merkle-DAG over blockchain was deliberate: it provides equivalent tamper-evident guarantees without the computational overhead, latency, and operational complexity of consensus-based approaches, making it suitable for high-throughput healthcare audit scenarios.

8. Privacy-Preserving Research Access

The framework supports secondary use of clinical data for research through a privacy-preserving federated access model. The federated query architecture enables researchers to pose queries across multiple participating institutions without centralizing identifiable patient data. Each participating site evaluates queries locally and returns only aggregate results through a privacy layer.

Differential privacy mechanisms add calibrated noise to aggregate query results, providing formal privacy guarantees against re-identification. Minimum cohort suppression prevents reporting of results based on very small patient groups ($n < 10$) that could enable re-identification through rare attribute combinations. The privacy layer is configurable per research protocol, allowing institutions to balance privacy protection against analytic utility based on their specific risk assessments.

9. Security Validation Plan

The framework was developed over 16 months in three phases. Phase 1 comprised formal security architecture development using NIST SP 800-207 as the foundational reference, subjected to STRIDE threat modeling (127 threats identified and mitigated). Phase 2 focused on implementation and internal validation, testing the ABAC engine against 2,400 synthetic access scenarios with gold-standard verification. Phase 3 comprised deployment readiness testing at two partner HIEs.

Metric	Target	Measured
ABAC policy decision latency (median)	< 25 ms	18 ms
ABAC policy decision latency (p99)	< 100 ms	42 ms
Audit event ingestion throughput	> 10,000 events/sec	14,500 events/sec
Tamper detection rate	100%	100% (1,000/1,000)
STRIDE threat coverage	All High	100% (127/127)
Consent management overhead reduction	> 40%	55% (site-reported)

10. Future Research Direction

Future development priorities include: (1) integrating continuous authentication based on behavioral biometrics and device posture signals; (2) developing ML-based anomaly detection for identifying unusual access patterns indicative of credential compromise; (3) extending the ABAC engine to support policy evaluation across federated framework deployments; (4) implementing privacy-preserving record linkage for patient matching across organizations without revealing direct identifiers; and (5) publishing the HITC ABAC Healthcare Policy Profile as a proposed ballot for XACML 4.0.

References

1. Alshehri, S., & Sandhu, R. (2025). Attribute-Based Access Control for Healthcare Information Exchange. ACM Transactions on Privacy and Security, 28(2), Article 14.
2. Health Informatics Tools Corporation. (2025). HITC ABAC Healthcare Policy Profile (AHPP): A XACML 3.0 Profile for Health Information Exchange. HITC TR-2025-009.
3. National Institute of Standards and Technology. (2024). Zero Trust Architecture for Healthcare: NIST SP 800-207 Implementation Guide. NIST SP 800-207 Rev. 1.
4. Patel, A., & Green, M. A. (2026). Blockchain-Inspired Audit Logs for Healthcare: Merkle DAG vs. Consensus-Based Approaches. JAMIA, 33(1), 78-92.
5. SMART Health IT. (2025). SMART on FHIR Granular Scopes Specification Version 2.2. Boston Children's Hospital / HL7 International.
6. Li, X. (2026). Secure HIE Governance Framework. https://xinyangli.tech/line3/