Security Architecture Reference
Zero Trust, PII/PHI, HIPAA Compliance
Healthcare Multi-Product Platform

This document defines the enterprise security architecture for healthcare platforms operating multiple product lines, enforcing Zero Trust Architecture (ZTA), protecting PII/PHI, and ensuring HIPAA compliance. Security is embedded by design across identity, network, application, data, analytics, and AI layers.

Security Architecture Principles

Never trust, always verify; Assume breach; Least privilege; Identity-first security; Data-centric controls; Encrypt everything; Audit everything; Automate enforcement; Human-in-the-loop for clinical risk; Compliance by design

Zero Trust Reference Architecture

User/System → Identity Provider → Policy Decision Point → Policy Enforcement Point → Resource
Continuous verification replaces network trust.

Identity & Access Management

OIDC/OAuth2, MFA, RBAC+ABAC, Conditional access, PAM, JIT access for admins and clinicians.

Network Security (ZTA-aligned)

Microsegmentation, private endpoints, east-west inspection, service mesh mTLS, egress controls.

Application Security Architecture

API gateway enforcement, token validation, secrets vault, secure coding, rate limiting, dependency scanning, SAST/DAST, policy as code.

Data Security for PII/PHI

Classification, encryption, tokenization, dynamic masking, access logging, retention enforcement, consent checks.

HIPAA Controls Mapping

Access control, audit controls, integrity, transmission security, authentication, minimum necessary access, breach notification via SIEM/SOAR.

Encryption & Key Management

TLS 1.2+, AES-256, HSM-backed KMS, rotation, envelope encryption, BYOK support.

Logging, Monitoring & SIEM

Centralized immutable logs for auth, data access, admin actions, API calls, AI usage.

Threat Detection & Response

EDR/XDR, UEBA, anomaly detection, ransomware detection, automated isolation and forensics.

DevSecOps Architecture

Shift-left scanning, IaC security, container scanning, secrets detection, no-scan-no-deploy policy.

Analytics, ML & GenAI Security

Row/column security, secure views, feature access control, model registry RBAC, GenAI gateway with RAG, validation, audit and human approval.

Third-Party & Vendor Security

BAAs, vendor risk reviews, token-based access, monitoring, data minimization.

Backup, DR & Ransomware Protection

Immutable backups, offline copies, automated restore testing, segregated admin access.

Governance, Risk & Compliance

Automated evidence generation, access reviews, change records, policy enforcement logs.

Security KPIs

PHI violations, MTTD/MTTR, encryption coverage, privileged access age, audit findings.

Why This Architecture Works

Provides end-to-end Zero Trust, automatic HIPAA compliance, safe analytics and AI, reduced blast radius, and audit readiness by default.