Standards, Governance & Guardrails for Team Self-Service
Healthcare Multi-Product Platform

This document defines the standards, governance model, and automated guardrails that enable engineering teams to self-serve infrastructure, applications, data, and AI capabilities while maintaining security, compliance, and architectural integrity in regulated healthcare environments.

Architecture Standards

Reference architectures, approved integration patterns, platform-first services, ADR-based decisions

Technology Standards

Approved cloud, CI/CD, observability, secrets, containers, data platforms

Data Standards

Data contracts, domain ownership, PHI classification, retention, certified metrics

Security Standards

Zero Trust, MFA, encryption, audit logging, tokenization, JIT access

Governance Model

Clear decision ownership, lightweight forums, mandatory artifacts, time-boxed exceptions

Automated Guardrails

Policy-as-code enforcing infra, app, data, security, and AI standards

Self-Service Capabilities

Teams provision infra, pipelines, data products, APIs, models, dashboards without tickets

Exception Handling

Business justification, mitigation, expiry, quarterly review

Metrics for Success

Provisioning time, reuse rate, violations, security findings, exception age

Operating Principles

Freedom inside guardrails, automation over approval, compliance by design