Healthcare Platform Architecture

HIPAA-Compliant Medical Records System

Core Components:

Patient Portal:	React app with biometric authentication
Provider Dashboard:	Angular app for healthcare providers
API Gateway:	AWS API Gateway with WAF
Identity Service:	Keycloak for SSO and RBAC
Patient Service:	Java Spring Boot - patient records
Appointment Service:	Python Django - scheduling
Medical Records Service:	Java Spring Boot - EHR management
Prescription Service:	Node.js - medication management
Billing Service:	Go - insurance claims processing
Audit Service:	Python - compliance logging
MongoDB:	Patient demographics (encrypted)
PostgreSQL:	Transactional data
S3 Bucket:	Medical imaging storage (encrypted)
AWS KMS:	Key management for PHI encryption

Critical Data Flows:

- Patient -> Portal -> API GW -> Identity Service (authentication)
- Portal -> Medical Records Service -> MongoDB (view records)
- Provider -> Dashboard -> Prescription Service (prescribe)
- Prescription Service -> External: Pharmacy Network API
- All Services -> Audit Service -> CloudWatch (compliance)
- Medical Records -> S3 (store imaging with encryption)

HIPAA Security Controls:

- PHI encrypted at rest (AES-256) and in transit (TLS 1.3)
- Role-based access control with minimum necessary access
- MFA required for all provider accounts
- Comprehensive audit logging for all PHI access
- Automatic session timeout after 15 minutes
- Data loss prevention (DLP) scanning
- Annual penetration testing and vulnerability assessments