HealthSync EHR Platform

System Design Document - HIPAA Compliant Architecture
Document Version: 2.1 | Last Updated: February 2025

1. System Overview

HealthSync is an enterprise Electronic Health Record (EHR) system serving 2,500+ healthcare providers across 180 facilities. The platform manages Protected Health Information (PHI) for over 12 million patients and processes 500,000+ clinical transactions daily. The architecture is designed for HIPAA compliance, HITRUST certification, and SOC 2 Type II requirements.

2. Core Architecture Components

Service	Technology Stack	Function	PHI Access
Patient Portal	React, Node.js, Express	Patient self-service, records access	Read-only PHI
Provider Workstation	Angular, .NET Core 8	Clinical documentation, orders	Full PHI access
Clinical API Gateway	Kong + AWS API GW	FHIR R4 API routing, throttling	Pass-through
Patient Demographics	Java 21, Spring Boot	Master patient index, registration	Demographics PHI
Clinical Documents	Python, FastAPI	Notes, reports, imaging metadata	Clinical PHI
Order Management	Java 21, Micronaut	Lab orders, prescriptions, referrals	Order PHI
Pharmacy System	C#, .NET 8	Medication management, e-prescribing	Medication PHI
Lab Integration Engine	Mirth Connect	HL7v2/FHIR lab interfaces	Lab results PHI
Imaging Gateway	Go, DICOM	PACS integration, image routing	Imaging PHI
Scheduling Service	Node.js, PostgreSQL	Appointments, resource management	Limited PHI
Billing Engine	Java, Oracle	Claims processing, coding	Billing PHI
Analytics Platform	Spark, Databricks	Population health, reporting	De-identified data

3. Critical Data Flows

3.1 Patient Registration Flow

Registration Desk → Patient Demographics Service → Identity Verification (Experian) → MPI Matching → Master Patient Index (PostgreSQL) → Insurance Eligibility Check (Availity) → Account Creation → Welcome Email (encrypted)

3.2 Clinical Documentation Flow

Provider Workstation → Clinical API Gateway (FHIR R4) → Clinical Documents Service → Document Storage (S3 encrypted) → Audit Log (immutable) → CDS Alerts Check → Real-time sync to Data Warehouse

3.3 E-Prescribing Flow (EPCS)

Provider Order Entry → Pharmacy Service → Drug Interaction Check (FDB) → Provider 2FA (DEA requirement) → Digital Signature (HSM) → Surescripts Network → Pharmacy Fulfillment → Patient Notification

3.4 Lab Results Flow

Reference Lab (Quest/LabCorp) → HL7v2 Message → Lab Integration Engine (Mirth) → FHIR Transformation → Results Repository → Provider In-basket Alert → Patient Portal Notification (with provider release)

4. HIPAA Security Controls

4.1 Access Controls (§164.312(a))

• Unique user identification with role-based access (RBAC) • Emergency access procedure with break-glass audit • Automatic logoff after 15 minutes of inactivity • Multi-factor authentication for all PHI access • Minimum necessary access enforcement

4.2 Audit Controls (§164.312(b))

• All PHI access logged with user, timestamp, patient, action • Audit logs retained for 7 years (immutable storage) • Real-time monitoring for suspicious access patterns • Monthly audit log reviews by Privacy Officer • Patient access reports available within 48 hours

4.3 Transmission Security (§164.312(e))

• TLS 1.3 for all external communications • VPN required for remote workforce access • End-to-end encryption for patient messaging • Secure email gateway for PHI transmission • SFTP with PGP for batch data transfers

5. Infrastructure Architecture

Component	Primary	DR Site	RPO/RTO
Application Tier	AWS us-east-1 (EKS)	AWS us-west-2 (EKS)	15 min / 4 hours
Database Tier	Aurora PostgreSQL Multi-AZ	Cross-region replica	5 min / 2 hours
Document Storage	S3 (SSE-KMS)	Cross-region replication	Near real-time / 1 hour
Identity Provider	Okta (HA)	Okta (multi-region)	N/A / 15 min
Message Queue	Amazon MQ (Active-Standby)	Replicated	0 / 30 min
CDN	CloudFront	Multi-region	N/A

6. External System Interfaces

• **HIE Connections:** CommonWell, Carequality - FHIR R4 document exchange

• **Lab Interfaces:** Quest, LabCorp, local hospital labs - HL7v2.5.1 / FHIR

• **Pharmacy Networks:** Surescripts (NCPDP SCRIPT 2017071) - EPCS certified

- **Imaging:** Local PACS systems - DICOM, DICOMweb
- **Insurance:** Availity, Change Healthcare - X12 270/271, 837/835
- **Public Health:** State immunization registries, CDC syndromic surveillance
- **Identity Verification:** Experian, LexisNexis - for patient matching