
Technical Specifications: ERP Core

1. Project Overview

- **Status:** Approved for Sprint 4 Development.
- **Objective:** The objective is to replace fragmented legacy systems with a unified data layer for hospital administration, reducing billing errors and optimizing supply chain latency.
- **Compliance:** Fully SOC2 Type II, HIPAA, and FHIR (Fast Healthcare Interoperability Resources) compliant.

2. System Architecture

The system utilizes a Federated Microservices Architecture. This architecture ensures that the pharmacy module can remain operational even if the billing or scheduling services are undergoing maintenance.

- **Integration Layer:** An HL7/FHIR-compliant engine that translates legacy HL7 v2 messages into modern JSON structures.
- **Core Services:** Independent containers for Patient Identity (MPI), Resource Scheduling, and Revenue Cycle Management (RCM).
- **Persistence Layer:** Encrypted-at-rest RDS for relational financial data and an immutable ledger for patient health record (PHR) audit trails.

3. Technical Implementation: The Patient Journey

3.1 Master Patient Index (MPI) Logic

To prevent duplicate records across multiple facilities, the MPI service uses a Probabilistic Matching Algorithm.

- **Weighting:** Assigns scores to Name, DOB, and SSN (last 4).
- **Thresholding:** Scores > 0.90 auto-merge; 0.70–0.89 flag for manual registrar review.

3.2 FHIR Resource Mapping

All clinical data must be exposed via the FHIR R4 standard.

Sample Patient Resource Mapping:

JSON

```
{
  "resourceType": "Patient",
  "id": "nh-99201",
  "active": true,
  "name": [{"family": "Smith", "given": ["Jane"]} ],
  "managingOrganization": { "reference": "Organization/hospital-alpha" }
}
```

4. Database Schema (Inventory & Pharmacy)

The inventory_ledger table tracks high-value medical devices and pharmaceuticals using RFID/Barcode integration.

Field	Type	Constraint
item_id	UUID	PK
lot_number	String	Indexed for recall tracking
expiration_date	Date	Trigger-enabled for alerts
stock_level	Integer	Atomic decrement on Dispense

5. Security & Infrastructure

- **Zero-Trust Access:** Every internal service request must be validated via an mTLS (Mutual TLS) certificate and a scoped JWT.
- **Audit Logging:** Every Read or Write of a Patient Resource is logged to an immutable, write-once-read-many (WORM) storage bucket for compliance audits.
- **Disaster Recovery:** Multi-region failover with a Recovery Point Objective (RPO) of < 5 minutes.

6. Integration Points (APIs)

6.1 Insurance Eligibility Verification

POST /api/v3/rcm/eligibility

- **Purpose:** Real-time 270/271 EDI transaction processing.
- **Payload:** Includes Provider NPI, Member ID, and Service Type Code.
- **Response:** Returns co-pay, deductible remaining, and authorization requirements.

7. Performance Benchmarks

- **EHR Search Latency:** < 150ms for patient lookups across 1M+ records.
- **Concurrency:** Support for 5,000+ simultaneous nursing station logins per cluster.
- **API Availability:** 99.99% (SLA-backed).

Implementation Notes for Developers:

1. Always use the Vault service for retrieving database credentials.
2. Never log PHI (Protected Health Information) to the standard application logs. Please use the SecureLogger utility.
3. FHIR Validation: All incoming payloads must pass the FHIR_Validator middleware before hitting the service logic.