THE OPEN GROUP®
INITIATE
Work Group

Project Title:

Enhancing Patient Care through IT: A Healthcare case

Team Name:

VisionArchiX

Course & Institution:

Faculty of Technology, University of Delhi

Mentor:

Ms. Reshma Nachnani

THE OPEN GROUP ®
INITIATE
Work Group

Table of Contents

Enterprise Architecture: Phase C – Information Systems Architecture Document

1. Introduction

Phase C of the TOGAF ADM framework focuses on the development of the **Information Systems Architectures**, comprising both the **Application Architecture** and the **Data Architecture**. In the context of AIIMS, this phase is instrumental in enabling the hospital to shift from siloed, legacy systems to a modern, integrated, and patient-centric digital health ecosystem. The core aim is to establish a robust IT backbone that supports high-quality, efficient, and secure healthcare delivery aligned with national initiatives such as the Ayushman Bharat Digital Mission (ABDM).

Phase C also acts as the strategic connector between the business goals outlined in Phase B and the enabling technologies to be detailed in Phase D. It provides a blueprint for digital transformation through clear architectural specifications of systems and data.

The scope of Phase C in the AIIMS transformation includes:

- Designing a unified, interoperable **Enterprise Application Stack** that covers EHR, Telemedicine, Lab Integration, Smart Ward Management, and Mobile Health Apps.
- Creating a secure and standards-compliant **Data Architecture**, enabling data-driven decision-making, real-time analytics, and integration with the National Digital Health Ecosystem (NDHE).
- Addressing challenges such as data fragmentation, inconsistent identifiers, manual workflows, and limited analytics capabilities.
- Laying the foundation for patient-centric innovations, such as AI-based diagnostics, patient portals, and seamless care transitions across departments and facilities.

2. Baseline Architectures

2.1 Baseline Application Architecture

The existing application landscape at AIIMS is characterized by **fragmented, department-specific software systems**, partial digitization, and lack of interoperability between core hospital functions. The technologies in use include legacy systems developed in-house, open-source experiments, and commercial solutions running in silos.

Current State Highlights:

- **Dual Hospital Information Management Systems (HIMS):** Operated in parallel in different wings or departments, leading to duplication of patient data and inconsistent workflows.
- **Departmental Tools:** Many departments (e.g., Radiology, Pathology, Surgery) use standalone tools such as local PACS (Picture Archiving and Communication System), LIS (Lab Information Systems), and pharmacy inventory systems.
- **Manual Operations:** Several functions including patient registration, OPD scheduling, referrals, and documentation are handled via paper or spreadsheets.
- **Appointment Scheduling Systems:** Existing systems do not prevent duplication or overlap, often causing long queues and patient dissatisfaction.
- **Academic Integration:** Student data, clinical rotations, and academic records are maintained separately, not integrated into the clinical systems.

Limitations and Challenges:

- **Siloed Systems:** Applications do not communicate, resulting in redundant data entry and fragmented patient records.
- **User Experience Issues:** Staff and clinicians must navigate multiple systems with inconsistent interfaces and authentication processes.
- **Scalability Issues:** The current systems were not designed for high-concurrency use or pandemic-level load management.

- **Mobile Accessibility:** Most systems are not mobile-friendly or responsive, severely impacting fieldwork, teleconsultation, and access on-the-go.
- **No API Layer:** Lack of APIs or service bus prevents integration with national digital health platforms (e.g., NDHM, eSanjeevani).

2.2 Baseline Data Architecture

The current data architecture lacks a unified and structured approach to healthcare information. Data resides in heterogeneous formats across multiple platforms, with no central data warehouse or governance policies in place.

Data Environment Observations:

- **Departmental Silos:** Each department maintains its own patient records, test results, and administrative data in isolation.
- **Unstructured & Semi-Structured Data:** Patient histories, lab results, prescriptions, and case summaries are stored in scanned PDFs, handwritten notes, or Word documents.
- **Absence of MPI:** There is no **Master Patient Index (MPI)** to uniquely identify and track patients across services, resulting in record duplication.
- **Disparate Identifiers:** Different departments use different formats for patient IDs, causing mismatches in clinical data and service delivery.
- **No Metadata Repository:** There is no inventory or cataloging of data elements, which limits interoperability and analytics capabilities.
- **Data Storage Issues:** Patient data is stored in ad hoc file systems or embedded databases (like MS Access, MySQL) on individual department servers.

Privacy & Security Gaps:

- **No Centralized Access Control:** Role-based or attribute-based access mechanisms are not consistently applied.
- **Lack of Encryption Standards:** Sensitive patient data is stored and transmitted without uniform encryption policies.
- **Limited Audit Trails:** Access to patient records is not fully logged or monitored for privacy breaches.
- **Regulatory Non-Conformance:** Incomplete alignment with HIPAA, GDPR, and NDHM data protection principles.

3. Target Architectures

3.1 Target Application Architecture

The Target Application Architecture envisions a **unified, scalable, interoperable, and patient-centric digital ecosystem** that supports seamless care delivery, operational efficiency, and decision intelligence across AIIMS.

Core Features & Components:

1. **Centralized Electronic Health Record (EHR) System**
   - Web-based, modular architecture
   - Real-time data entry and access for OPD, IPD, Emergency, Labs, and Pharmacy
   - Integrated clinical decision support (CDS) tools

2. **Telemedicine Platform**
   - AI-enabled triage, appointment management, video consultations
   - Integration with ABHA/Health ID, consent management
   - Post-consultation e-prescription, follow-up scheduling

3. **Smart Ward & IoT Integration**
   - Vital sign monitors, smart beds, and environmental sensors
   - Real-time alerts to nurses/clinicians via mobile dashboards
   - Integration with centralized alerting and monitoring system (Node-RED/Kafka)

4. **Mobile and Web Portals**
   - **Patient Portal**: View prescriptions, reports, upcoming visits, consent logs
   - **Staff Portal**: Bed management, diagnostics orders, shift tasks
   - Designed for multilingual, low-bandwidth, mobile-first usability

5. **Academic and Research Modules**
   - Digital logbooks for students and interns
   - Research data management integration with publication tools

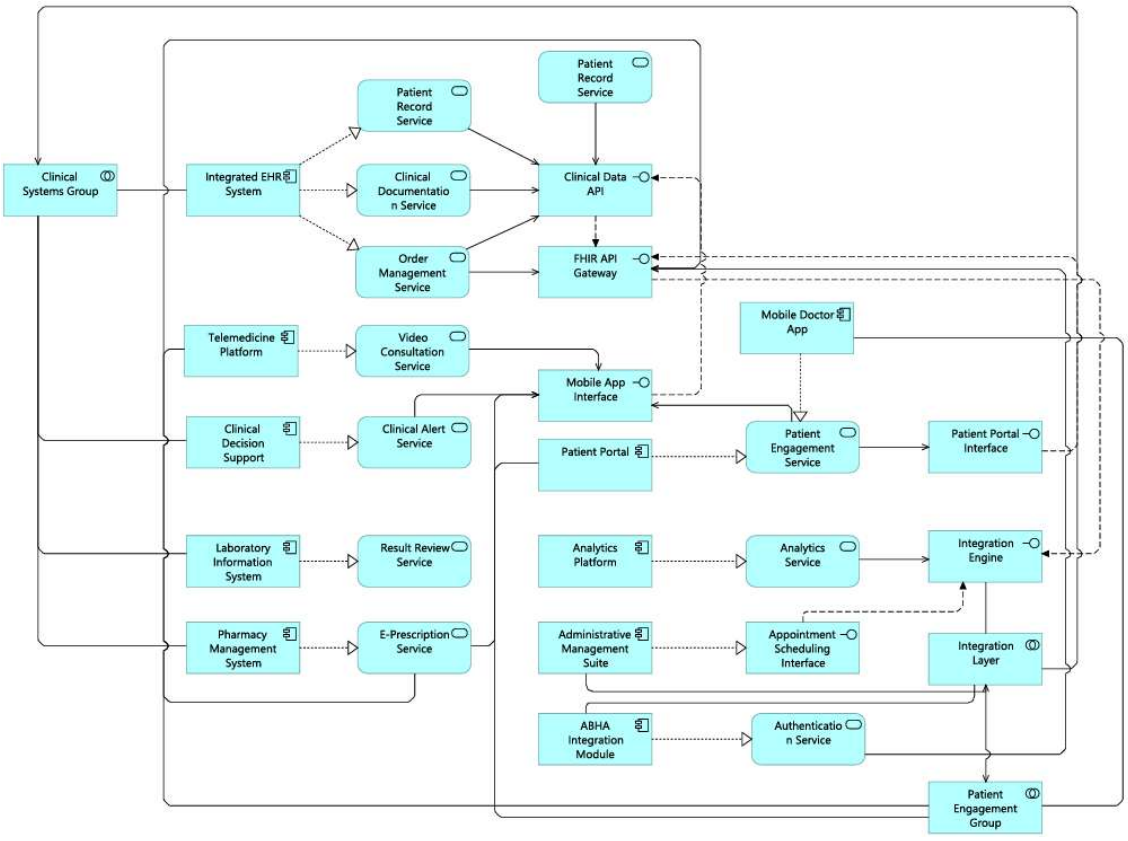
6. **Academic and Research Modules**
   - API Gateway with support for REST, HL7v2, and FHIR R4 protocols
   - Enterprise Service Bus (ESB) or Kafka-based event-driven architecture
   - Middleware for connecting with NDHM platforms (eSanjeevani, HFR, HIE-CM)

7. **Legacy System Connectors**
   - Adapter modules for Lab, Pharmacy, and Radiology Systems
   - Gradual migration support for legacy database schemas

Key Capabilities Supported:

Capability	Application Enabler
Patient 360° View	Unified EHR + MPI + Consent Dashboard
Remote Consultations	Telemedicine App + NDHM Gateway Integration
In-Patient Monitoring	IoT Smart Ward App + Alert Manager + Real-time Dashboard
Real-Time Bed Tracking	Staff Portal + Hospital Command Centre Interface
Academic & Clinical Sync	Research Data Warehouse + Student Portal

3.1.1 Application Architecture Diagram



3.2 Target Data Architecture

The Target Data Architecture focuses on building a **centralized, standards-compliant, and secure data foundation** that powers clinical workflows, strategic analytics, and regulatory reporting.

Core Data Architecture Components:

1. **Healthcare Data Lake**
   - Consolidates structured and unstructured data across departments

- Supports real-time ingestion and batch ETL from legacy systems
- Hosted on hybrid cloud (Gov Cloud + On-Prem)

2. **Enterprise Data Warehouse (EDW)**
   - Normalized schema for longitudinal health records
   - Powers dashboards for hospital administration, research, and policymaking
   - OLAP cubes for advanced reporting and forecasting

3. **Master Patient Index (MPI)**
   - ABHA/Health ID integration with fuzzy matching logic
   - Deduplication, merge rules, and consented data sharing
   - Central identity resolution across OPD, IPD, Labs, Pharmacy

4. **Role-Based Access Control (RBAC)**
   - Based on user profiles: Clinician, Nurse, Pharmacist, Researcher, Admin
   - Attribute-based extensions for dynamic policy enforcement
   - Integrated with Keycloak (or similar IAM platform)

5. **Data Interoperability Standards**
   - HL7 v2 for legacy systems
   - HL7 FHIR R4 for new APIs and exchange
   - SNOMED-CT, LOINC, and ICD-11 for clinical vocabularies

6. **Secure Data Lifecycle Management**
   - End-to-end encryption (AES-256, TLS 1.3)
   - Retention, archival, and anonymization policies based on data classification
   - Metadata cataloging and tagging for searchability and traceability

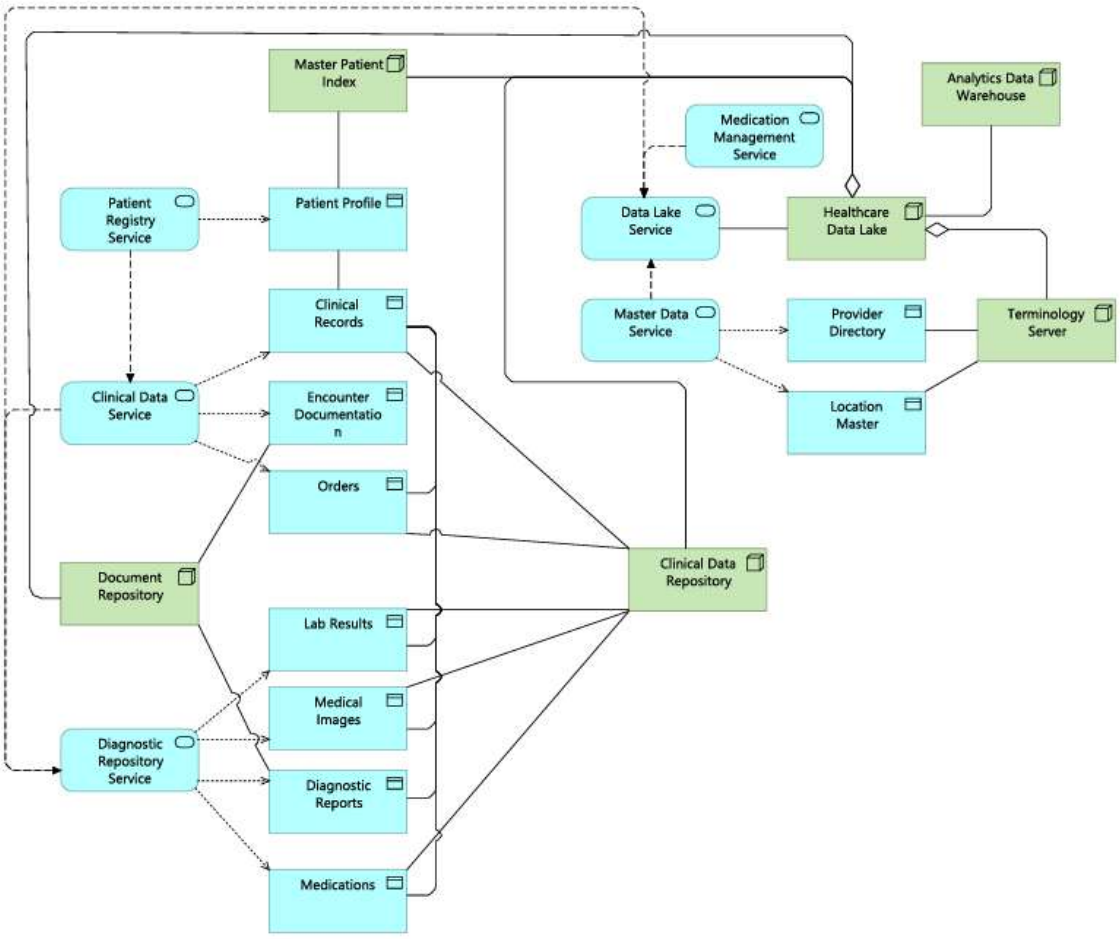
7. **Consent and Audit Framework**
   - Consent Manager compliant with NDHM specifications
   - Immutable audit trails (blockchain-ready optionality)
   - User activity logging and alerting

Key Data Use Cases Supported:

Use Case	Data Architecture Element
Predictive Risk Scoring	EDW + ML Pipelines on historical patient data
ABHA-Federated Data Sharing	MPI + API Gateway + Consent Manager
Hospital Performance Dashboards	EDW + Departmental ETL connectors
AI Training Datasets	Data Lake with pseudonymized structured records

National Health Registry Sync	Interoperability Layer + HL7/FHIR APIs

3.2.1 Data Architecture Diagram



4. Architecture Models

This section defines the architecture models needed to represent the **interaction, deployment, and data behavior** of applications and systems at AIIMS. These models help validate whether the target architecture can meet the business and technical requirements identified in Phases B and C.

4.1 Application Communication and Integration Models

This model shows how various application modules interact with each other and with external systems.

4.1.1 Internal System Interactions:

- **EHR ↔ Lab/RIS/PACS:** Using HL7 v2 for legacy labs and FHIR for modern diagnostic APIs.
- **EHR ↔ Pharmacy Management System:** Prescription sync, drug inventory check, refill alerts.
- **EHR ↔ Appointment & Triage Module:** To allocate slots, fetch patient history, suggest clinician.
- **EHR ↔ Smart Ward Apps:** Vital signs updates pushed every 5 minutes to patient timeline.
- **Student/Academic Portal ↔ Research Data Lake:** Controlled access for academic insights.

4.1.2 External Integration Points:

- **NDHM Gateway:** For ABHA sync, consent verification, HIE-CM integration.
- **eSanjeevani Platform:** For teleconsultation integration and interoperability.
- **Health Facility Registry & HRP:** For automated updates on infrastructure and resource availability.

**All communication is routed through an API Gateway with secure tokens, throttling, and audit logs.*

4.2 Application Deployment Models (Cloud-Native Microservices)

The system will be deployed using a **containerized microservices architecture**, orchestrated via Kubernetes on a **hybrid cloud setup** (Gov Cloud + AIIMS private data centers).

Deployment Architecture Layers:

1. **Presentation Layer:**
   - React Native mobile apps (Patients, Doctors)
   - Web frontends (Admin, Nurse Station, Labs)

2. **Application Layer:**
   - REST APIs built using Node.js and Spring Boot
   - Services containerized using Docker
   - Managed by Kubernetes with auto-scaling enabled

3. **Integration Layer:**
   - Kafka Event Bus for asynchronous event communication
   - HL7/FHIR Transformers for standards-based exchange

4. **Data Layer:**
   - PostgreSQL for transactional databases
   - S3-compatible object storage for files/images

- Hadoop/Spark cluster for analytics and ML

5. **Security & Observability Layer:**
   - Keycloak for IAM
   - Prometheus + Grafana for performance
   - ELK Stack for centralized logging

** Zero-downtime rolling updates, disaster recovery replication, and fault-tolerant pods are configured.*

4.3 Data Flow and Entity Relationship Diagrams (ERDs)

4.3.1 Data Flow Diagrams (DFD):

- **Patient Journey:** From registration → diagnosis → lab orders → medication → discharge → follow-up
- **Real-Time Alerts:** Vitals → IoT Gateway → Alert Broker → Nurse Dashboard + Doctor Mobile App
- **ABHA-Federated Data Exchange:** Local EHR → Consent Engine → NDHM API → Federated node

4.3.2 Entity-Relationship Diagram

**ERDs follow the OpenEHR archetype for clinical modeling to ensure future interoperability.*

4.4 CRUD Matrix (Applications vs. Data Entities)

This matrix shows how each application component interacts with core data entities.

Data Entity	EHR	Lab/RIS	Pharmacy	Consent Manager	Analytics	Research Portal
Patient Profile	C/R/U/D	R	R	C/R/U/D	R	R
Encounter Notes	C/R/U/D	—	—	—	R	R
Lab Orders	C/R	C/R/U/D	—	—	R	—
Prescriptions	C/R/U	—	R/U/D	—	R	—
Consent Records	—	—	—	C/R/U/D	R	—

Vitals/IoT Logs	—	—	—	—	R	R

C = Create, R = Read, U = Update, D = Delete
Note: Operations are restricted based on RBAC policy.

5. Architecture Building Blocks (ABBs) & Solution Building Blocks (SBBs)

This section identifies and describes the core Architecture Building Blocks (ABBs) required to meet AIIMS' target application and data architecture objectives. Each ABB is mapped to one or more Solution Building Blocks (SBBs) that reflect real-world products, tools, or implementations being considered or already in use.

5.1 Application ABBs and Corresponding SBBs

These building blocks define the foundational systems and modules that collectively constitute the enterprise application architecture for AIIMS.

Application ABB	Purpose	Solution Building Block (SBB)	Notes
Centralized EHR System	Unified clinical record management	OpenMRS, Bahmni, Medix (custom)	Modular open-source platform with HL7/FHIR support
Patient Registration and MPI	Unique identity resolution, registration across departments	ABHA-integrated MPI engine + Custom Registration UI	ABHA (NDHM) compliance with fuzzy matching logic
Appointment & Scheduling System	Multi-department, doctor, and lab appointment management	BookMyOPD-like workflow; React frontend with PostgreSQL backend	Calendar sync, auto-load balancing, triage support
Telemedicine Gateway	Remote consultation, follow-ups, video calling	eSanjeevani integration + Jitsi-based interface	Supports NDHM Consent Manager and E-prescriptions

Pharmacy Management System	Drug inventory, dispensing, refill tracking	Odoo ERP Module, or OpenBoxes	Custom role-based workflows for controlled substances
IoT-Integrated Smart Ward System	Real-time vitals monitoring and alerts	Node-RED + MQTT Broker + Custom Dashboard	Integrated with nursing stations and alerting logic
Laboratory Information System (LIS)	Test order management, results entry, and reporting	OpenELIS or LabWare with HL7 connectors	Plug-and-play with Radiology and Pathology
Clinical Decision Support (CDS)	Rule-based alerts and predictive suggestions	OpenCDS with AI plugin integration	Triggers based on lab, vitals, or diagnosis criteria
Patient Portal (Web/Mobile)	Patient-facing access to records, appointments, and consent	React Native + OAuth2 (Keycloak) + GraphQL backend	Integrates health summary, reports, invoices, and follow-ups
Academic & Research Portal	Research data access, clinical learning management	REDCap + Moodle Integration	Access-controlled environment for students and researchers

5.2 Data ABBs and Corresponding SBBs

These building blocks ensure the management, structuring, protection, and meaningful use of clinical and administrative data across AIIMS.

Data ABB	Purpose	Solution Building Block (SBB)	Notes
Healthcare Data Lake	Central repository for structured and unstructured data	Hadoop/Spark cluster or Azure Data Lake	Supports real-time and batch ingestion from legacy and new systems
Enterprise Data Warehouse (EDW)	Normalized data warehouse for analytics and reporting	PostgreSQL-based OLAP + Power BI or Apache Superset	Star/snowflake schema design for scalability
Master Patient Index (MPI)	Unified patient identification across systems	ABHA-integrated MPI + PostgreSQL + Fuzzy Matching Algorithm	Core to patient-centric design and NDHM interoperability
Consent Management System	Manage data access preferences and patient privacy	NDHM HIE-CM compliant service +	Logs all requests, grants, and revocations

		blockchain-ready audit module	
Metadata Repository	Catalog data models, definitions, lineage	Apache Atlas or Amundsen	Enables data discoverability and governance
Role-Based Access Control (RBAC)	Enforce access rules across systems and users	Keycloak + Open Policy Agent (OPA)	Supports fine-grained access and external policy configuration
Audit Logging and Monitoring	Capture access logs and unusual behavior	ELK Stack (Elasticsearch, Logstash, Kibana) + Prometheus	Centralized dashboard with alert triggers and SIEM integration
Data Interoperability Layer	Translate data between systems and standards	HL7 v2 → FHIR API transformers using HAPI-FHIR + Kafka	Supports JSON/XML payload conversion and secure exchange

5.3 ABB-to-SBB Mapping Overview

Domain	ABB	Mapped SBBs
Applications	EHR, Scheduling, Smart Ward	OpenMRS, Bahmni, Node-RED, React, Kafka
Data	Data Lake, MPI, Consent	Hadoop/Spark, PostgreSQL, NDHM APIs
Security	RBAC, Logging	Keycloak, OPA, ELK
Interoperability	HL7/FHIR Adapters	HAPI-FHIR, Kafka, API Gateway (Kong/Zuul)
Analytics	Research and BI Systems	Power BI, Apache Superset, REDCap

6. Gap Analysis

The purpose of this section is to identify and assess the **gaps** between the Baseline and Target Architectures across both **Application and Data domains**, classify their criticality, and propose remediation strategies aligned with enterprise goals and constraints. This serves as a foundation for defining transition architectures and informing the implementation roadmap in later phases.

6.1 Identified Gaps in Application Functions

Application Area	Baseline Limitation	Target Requirement	Gap Description	Priority
Electronic Health Records	Dual HIMS with partial digitization	Unified, interoperable EHR with full patient lifecycle support	Fragmentation, data duplication, lack of workflow consistency	High
Appointment Scheduling	Manual or siloed scheduling with overlaps	Centralized, conflict-free, patient-accessible scheduling	Inefficiencies, delays, no patient interface	High
Telemedicine	Limited or pilot-based; disconnected from core records	Full-featured teleconsult platform integrated with EHR and ABHA	Lack of scalability, integration, and workflow alignment	Medium
Clinical Decision Support	Not available in current systems	Embedded real-time CDS alerts and AI-based decision aids	Absence of data-driven triage or recommendations	Medium
Mobile App Access	Not supported or extremely limited	Mobile/web portals for patients and staff	No mobile accessibility to health records or appointments	High
Academic & Research Systems	Disconnected research systems, no linkage to EHR or analytics	Integrated portals for research queries and anonymized datasets	Siloed data limits cross-functional research	Medium

6.2 Identified Gaps in Data Capabilities

Data Capability	Baseline Condition	Target Capability	Gap Description	Priority
Master Patient Index (MPI)	No centralized identity or consistent	Unified MPI linked with ABHA	Data duplication, reconciliation	High

	patient ID across departments		issues, fragmented histories	
Interoperability	No HL7/FHIR layer, manual exchanges between departments	FHIR-compliant data exchange across systems	Inability to sync in real time or exchange with NDHM	High
Real-Time Data Availability	Reports and labs manually uploaded, delays in availability	Near real-time updates to EHR, dashboards, and analytics engines	Clinical delays, outdated decision support	High
Metadata & Data Governance	No metadata repository, inconsistent schema definitions	Central metadata catalog, version control, and lineage tracking	Low data quality, lack of standardizatio n	Medium
Consent Management	Manual consent, or absent beyond paper forms	Digital consent manager, integrated with NDHM	Non-compliance, patient mistrust, and audit limitations	High
Analytics and AI Enablement	No data warehouse, data lake, or training pipelines	Healthcare Data Lake + ML-ready datasets	Poor decision-making ability, lack of predictive capacity	

6.3 Gap Prioritization & Remediation Strategy

Gap Prioritization Matrix

Impact Area	Urgency	Complexity	Remediation Approach	Phase
Unified EHR System	High	High	Replace dual HIMS with OpenMRS-based unified stack	Transition Arch 1

Master Patient Index	High	Medium	Deploy ABHA-integrated MPI and reconcile existing IDs	Transition Arch 1
Scheduling System	High	Low	Implement scalable scheduling module with triage logic	Transition Arch 1
HL7/FHIR Integration	High	Medium	Setup integration engine with HAPI FHIR and Kafka bus	Transition Arch 2
Consent Management	High	Medium	Use NDHM-compatible Consent Manager + ABHA sync	Transition Arch 2
Data Analytics Enablement	Medium	High	Establish Data Lake and Data Warehouse foundation	Transition Arch 3
Mobile & Patient Portals	Medium	Low	Develop React Native apps with RBAC backend	Transition Arch 2

7. Impact Assessment

This section evaluates the **consequences** of transitioning from the current to the target state across technical systems, organizational workflows, stakeholder roles, and regulatory boundaries. These impacts must be considered for effective change management and to design a realistic, sustainable implementation roadmap.

7.1 Technical Impacts

The shift to a modernized, integrated architecture introduces several **infrastructure and architectural transformation challenges**:

Key Technical Changes and Implications:

Area	Current State	Target Impact
System Architecture	Monolithic or siloed systems	Microservices deployment requires orchestration (e.g., Kubernetes)
Infrastructure Footprint	On-premise servers with static configurations	Migration to hybrid cloud requires new monitoring and scaling tools
Interoperability	No integration standards	Requires HL7/FHIR APIs, integration engine, API management gateway
Deployment Automation	Manual deployment processes	CI/CD pipelines needed for rapid, repeatable releases
Data Volume & Velocity	Periodic entry and uploads	Real-time ingestion and analytics demand new data pipelines
IAM & RBAC	Departmental logins with minimal controls	Unified IAM layer (Keycloak) and policy enforcement across applications
System Integration	Point-to-point connections	Event-driven architecture via Kafka adds complexity and governance

7.2 Stakeholder Impacts

Organizational and human factors are critical for successful adoption. These changes will alter responsibilities, workflows, and training needs across all stakeholder groups.

7.2.1 Clinicians & Nurses

- **Impact**: Shift from paper/manual workflows to structured digital records, real-time alerts, and EHR-based prescriptions.
- **Mitigation**: Tailored training modules, change champions in each department, hands-on sandbox environments.

7.2.2 Administrative Staff

- **Impact**: New digital tools for registration, billing, referrals, and audit logging.
- **Mitigation**: Provide dashboard training, SOP realignment, and process simulation runs.

7.2.3 IT Team

- **Impact**: Responsibility expands to include orchestration, cloud deployment, API management, security compliance, and monitoring.
- **Mitigation**: Upskill in DevOps, HL7/FHIR protocols, cloud administration (AWS/NIC Cloud).

7.2.4 Patients

- **Impact**: More digital touchpoints – online appointments, report access, consent controls.
- **Mitigation**: Multilingual tutorials, assisted digital kiosks, feedback loops for early usability issues.

7.2.5 Students & Researchers

- **Impact**: Easier access to structured, anonymized data; digitized academic workflows.
- **Mitigation**: Controlled sandbox access and documentation for ethical use and protocol adherence.

7.3 Regulatory & Security Considerations

Given the sensitive nature of health data and AIIMS' alignment with national digital health infrastructure, regulatory adherence and cybersecurity readiness are paramount.

Key Regulatory Impacts:

Domain	Requirement	Design Response
HIPAA / GDPR	Patient consent, data minimization, right to erasure	Consent engine, ABHA-linked ID, data lifecycle tagging
NDHM (ABDM)	Health ID usage, facility registry, digital consent, FHIR APIs	NDHM Gateway Integration, consent log system, FHIR-first APIs
IT Act, India	Data localization, security controls, breach reporting	Hybrid cloud with regional storage zones and encrypted backups
Audit & Monitoring	Continuous tracking of access, modifications, and exceptions	Immutable audit logs via ELK Stack + anomaly detection
Security Protocols	TLS encryption, secure token handling, zero trust architecture	Role + Attribute Based Access Control (RBAC + ABAC), end-to-end TLS

7.4 Operational Readiness & Transition Risk Factors

Risk Area	Potential Challenge	Mitigation Strategy
Staff Adoption	Resistance to change or digital fatigue	Role-based training, incentives, early adopters as evangelists
System Downtime	Transition causing outages	Phased deployment + rollback plans + dry-run simulations
Legacy Integration Complexity	Adapters required for labs, HR, and finance systems	Build and test integration bridges in sandbox first
Data Migration Accuracy	Risk of data loss or mismatch during transformation	Deduplication scripts, dry-run validations, manual override windows
Budget Overruns	Underestimation of infrastructure or licensing costs	Stage-wise budgeting, open-source preference, TCO modeling

8. Re-Use and Interoperability Assessment

This section assesses the potential for **reusing existing application and data components**, both within AIIMS and across the broader national health ecosystem. It also evaluates how well the proposed architecture supports **interoperability** with internal systems, external platforms, and national initiatives like NDHM/ABDM.

8.1 Potential for Re-Use of Existing Systems and Open Standards

The architecture consciously promotes the reuse of existing technology assets, open-source platforms, and standardized frameworks to reduce cost, accelerate deployment, and ensure maintainability.

8.1.1 Internal (AIIMS) Reuse Opportunities

Component	Current State	Reuse Strategy
Existing PACS/RIS	Functioning in Radiology and Cardiology	Integrate with HL7 interface layer and retain backend where stable
Lab Order Modules	Partially digitized in some departments	Enhance and plug into new LIS interface with mapped identifiers

Appointment Workflows	Manual but well-understood operational logic	Digitize current SOPs into scheduling app with rule engines
Data Entry Interfaces	Familiar forms in OPD/IPD systems	Adapt form fields/layouts into new EHR UI to reduce training time

8.1.2 Open-Source and Industry-Standard Reuse

Asset	Purpose	Why Reuse is Viable
OpenMRS/Bahmni	Core EHR and modular clinical workflows	Extensible, field-tested in India (e.g., Jharkhand, Karnataka)
OpenELIS	Lab Information Management System	Compatible with HL7, modular for customization
Keycloak	IAM & RBAC	Widely used in healthcare, integrates with OAuth2/OIDC
HAPI FHIR	HL7/FHIR API Layer	Community-supported, supports NDHM compliance
Node-RED	Workflow & IoT logic	Lightweight, visual tool already used in clinical automation pilots
Apache Kafka	Messaging & Event Streaming	Robust integration layer, supports decoupled microservices
REDCap	Research data collection	HIPAA-compliant, popular in academic hospitals

These reusable components reduce vendor lock-in, leverage community knowledge, and support faster prototyping.

8.2 Interoperability with Government Platforms and External Systems

The Target Architecture is designed to comply with interoperability mandates from the **Ayushman Bharat Digital Mission (ABDM)** and can interface with other government and public healthcare platforms through standardized protocols.

8.2.1 NDHM/ABDM Integration Targets

Platform	Integration Objective	Architecture Design Strategy

ABHA/Health ID System	Use as primary patient identifier across all modules	MPI integrated with ABHA registry and ABHA-linked login support
HIE-CM (Health Information Exchange – Consent Manager)	Exchange of clinical data across institutions based on patient consent	API layer + consent engine + audit logs using blockchain-ready logs
Health Facility Registry (HFR)	Maintain AIIMS hospital and facility profile	Auto-publish metadata via API updates from internal inventory
eSanjeevani Telemedicine	Allow shared case workflows and consultation scheduling	NDHM-certified APIs, integrated triage with AIIMS telemedicine
DigiLocker / NDHB Repositories	Provide downloadable patient reports and prescriptions	Consent-based document upload + push to DigiLocker when opted-in

All integrations follow HL7 v2/FHIR R4 standards and are deployed behind an API Gateway with JWT-based authentication.

8.3 Internal Interoperability Strategy

Challenges Addressed:

- Departmental silos in Radiology, Pharmacy, Labs
- Disconnected master data (patients, providers, inventory)
- Custom legacy file formats (e.g., CSV, PDF scans)

Interoperability Design Features:

- **API Gateway Layer:** Centralized access point with version control and load balancing
- **FHIR Transformers:** HL7 v2 → FHIR mapping modules for legacy system compatibility
- **Unified Event Bus:** Kafka streams connecting modules for real-time updates (e.g., new lab results triggers alert)
- **Metadata-Driven ETL Pipelines:** For lab, pharmacy, and billing data normalization

9. Data Security and Privacy Strategy

Effective data security and privacy are foundational to the AIIMS digital transformation, given the sensitivity of health records, the regulatory environment (HIPAA, GDPR, NDHM), and the institutional responsibility AIIMS bears as a premier government hospital. This strategy ensures that data is **protected, traceable, controlled, and ethically managed** throughout its lifecycle.

9.1 Privacy Policies and Consent Management

The architecture enforces a **"Privacy by Design"** approach, ensuring that patient rights, data ownership, and transparency are embedded into every layer of the application and data architecture.

Key Privacy Policies:

- **Data Minimization**: Only necessary data elements are collected for clinical, research, or administrative purposes.
- **Explicit Consent**: Patients must provide informed, granular, and revocable consent before any data sharing.
- **Right to Access and Erasure**: Patients can view, download, and request deletion of their data as per policy.
- **Purpose Limitation**: Data is only used for stated and agreed-upon clinical or research intents.

Consent Management Implementation:

- **NDHM-Compliant Consent Manager** integrated with ABHA (Health ID) ecosystem.
- Patient-facing **Consent Dashboard** (via mobile/web) to manage approvals and view data access history.
- **Audit logs** generated for every data access/modification involving patient information.
- Real-time integration with **Health Information Exchange – Consent Manager (HIE-CM)** for federated care exchange.

9.2 Encryption and Access Control Standards

The architecture ensures that all data – at rest, in transit, and in use – is encrypted using industry-grade algorithms and controlled through strict identity management.

Data Encryption Protocols:

Layer	Standard Used	Description
Data at Rest	AES-256	Applied to databases, file stores, logs
Data in Transit	TLS 1.3 + Mutual TLS (mTLS)	Between microservices, API Gateway, and external platforms

API Security	OAuth 2.0 + JWT	Token-based authentication for all API requests
Disk Encryption	LUKS + Hardware-level support (where available)	Protects backup media and offline data storage

Access Control and IAM:

- **Keycloak** as centralized Identity and Access Management (IAM) solution.
- **Role-Based Access Control (RBAC)**: Access granted based on professional role (doctor, nurse, lab tech, admin).
- **Attribute-Based Access Control (ABAC)**: Additional filters based on context like location, department, time.
- **Multi-Factor Authentication (MFA)**: Enforced for all admin roles and remote access.

9.3 Monitoring, Auditing, and Incident Response

Real-time detection and response mechanisms are critical for ensuring that breaches are not only prevented but also detected, analyzed, and addressed quickly.

Security Monitoring Infrastructure:

- **SIEM Platform**: Integrated ELK Stack + Wazuh/OSSEC for centralized log collection and threat detection.
- **Anomaly Detection**: Baseline behavioral analytics to flag unusual access patterns or privilege escalations.
- **Immutable Audit Trails**: All access, edits, exports, and consents are logged with tamper-evident timestamps.
- **Data Classification Engine**: Auto-labels sensitive, confidential, and public data for appropriate protection.

Incident Response Protocol:

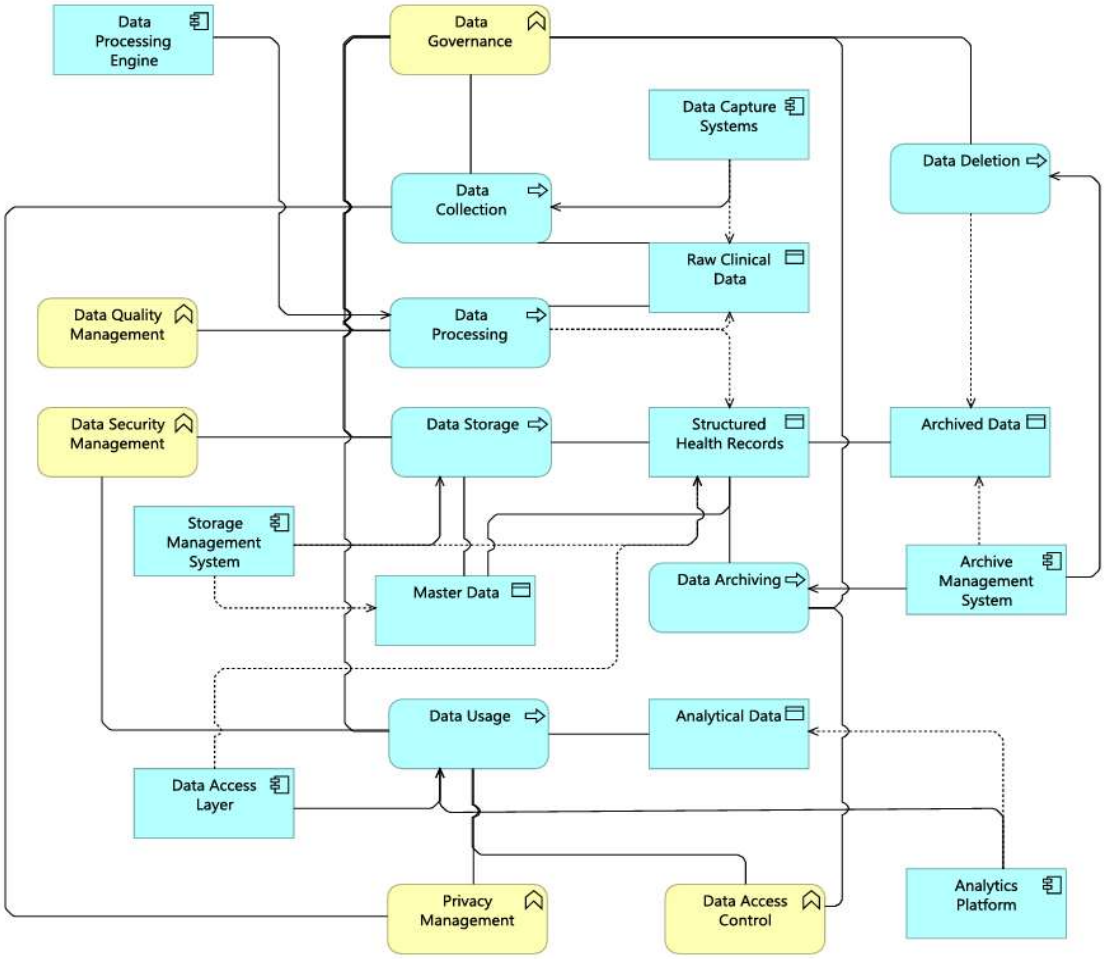
- Defined **playbooks** for common incidents (e.g., credential misuse, unauthorized export).
- Incident escalation matrix involving IT security, legal, medical records, and compliance teams.
- **Regulatory Notification Workflow**: GDPR and HIPAA timelines enforced for breach reporting (within 72 hrs).
- **Post-incident reviews and patches** integrated into DevSecOps pipelines.

9.4 Data Lifecycle & Retention Governance

Data management policies are tailored for healthcare-specific timeframes and legal mandates in India.

Data Type	Retention Period	Archival Strategy
Patient Clinical Records	10+ years (per NDHM/ICMR)	Archived to secure cold storage (encrypted)
Radiology & Lab Reports	5–10 years	Compressed DICOM/pdf archived in data lake
Research & Academic Records	15+ years (subject to ethics)	Pseudonymized and retained for reproducibility
Consent Logs & Access Trails	7 years	Stored in immutable, audit-only storage

9.4.1 Data Lifecycle Diagram



9.5 Regulatory Compliance Alignment

Regulation	Requirement	Implementation Strategy
HIPAA (US)	Confidentiality, Integrity, and Availability (CIA)	RBAC, audit trails, encrypted backups, incident response framework
GDPR (EU)	Right to Access, Erasure, Data Portability	Consent manager + download/export options for patients
NDHM/ABDM	Health ID, consent, digital exchange via FHIR APIs	NDHM Gateway, ABHA-linked MPI, Consent Layer
IT Act (India)	Reasonable security practices	SIEM, periodic penetration testing, endpoint hardening

10. Compliance Mapping

This section maps the AIIMS Target Information Systems Architectures against relevant **legal, regulatory, and interoperability compliance frameworks**, ensuring that all architectural decisions contribute to a secure, ethical, and standardized healthcare delivery environment. Compliance is especially critical as AIIMS transitions into a **model institution for NDHM alignment and global digital health partnerships**.

10.1 Core Compliance Domains and Frameworks

Regulatory/Standards Body	Domain	Applicability to AIIMS
NDHM / ABDM (India)	National Digital Health Interoperability	ABHA (Health ID), FHIR APIs, Consent Management, HFR
IT Act 2000 & SPDI Rules	Indian IT & Data Protection Law	Security practices, breach response, data storage requirements
HIPAA (US)	Health Information Privacy & Security	For international collaborations, research, and data handling ethics
GDPR (EU)	Data Protection & Subject Rights	Required for partnerships with EU universities, researchers
HL7/FHIR Standards	Interoperability & Data Exchange	Industry standard for APIs, health data formats
LOINC / SNOMED-CT / ICD-11	Clinical Terminologies	Standardized diagnostics, observations, and condition coding

10.2 Detailed Compliance Mapping Table

Compliance Area	Requirement	AIIMS Strategy / Design Response
NDHM - ABHA Integration	Unique, interoperable Health IDs across systems	MPI system integrated with ABHA APIs and token-based validation
NDHM - Consent Management	Federated data sharing based on explicit consent	NDHM-compliant Consent Manager with audit logs and revocation support
NDHM - HFR Registry	Mandatory facility registration with metadata updates	Automated sync with HFR via API using Facility Master Data
HIPAA - Data Confidentiality	Access control, encryption, audit trails	RBAC/ABAC enforcement + TLS + centralized logging (ELK, Wazuh)
HIPAA - Breach Notification	Incident reporting within 60 days of detection	Defined response playbooks, breach dashboard, legal escalation protocol
GDPR - Right to Erasure	Patients can request deletion of personal data	Consent & Privacy Dashboard allows patient-initiated delete requests
GDPR - Data Portability	Structured export of personal health data	Downloadable FHIR/JSON summary from EHR and consent manager
IT Act - Reasonable Security Practices	Periodic testing, controls, policies	Vulnerability scans, endpoint hardening, SIEM alerts, data encryption
FHIR (R4)	Standardized patient/encounter/diagnosis data APIs	All new APIs are FHIR R4-based with versioning & validation layer
HL7 v2	Backward compatibility for lab/PACS/RIS systems	HL7-to-FHIR transformers in Kafka integration layer
LOINC / SNOMED / ICD-11	Standard vocabulary for labs, clinical data, conditions	Terminology service layer with concept mapping engine

10.3 Compliance Validation and Certification Approach

1. Internal Compliance Framework

- Mapping each architectural artifact (e.g., API spec, data schema, user flow) to a compliance checklist
- Periodic internal audit using custom checklists derived from HIPAA, NDHM, GDPR
- Involvement of IT security, legal, medical, and administrative domains

2. Certification and Conformance Testing

- NDHM Sandbox Testing for ABHA, Consent Manager, HFR APIs
- Validation through automated FHIR API validators (e.g., Inferno, Touchstone)
- Readiness for NABH (National Accreditation Board for Hospitals) digital maturity assessment

3. Logging and Reporting

- Immutable audit logs retained for 7 years
- Patient-accessible consent and access logs (as per GDPR and NDHM norms)
- Breach reporting system tied to internal legal & security team workflows

10.4 Continuous Compliance Monitoring Strategy

Mechanism	Purpose
Security & Compliance Dashboard	Real-time visibility into regulatory KPIs
Policy-as-Code Enforcement (OPA)	Dynamic enforcement of data access rules
Penetration Testing (Quarterly)	Vulnerability management and threat detection
Compliance Heat Maps	Identify compliance coverage and areas of risk
Incident & Breach Drill Logs	Preparedness tracking and accountability chain

11. Transition Architectures

Transition Architectures define intermediate states that bridge the gap between the Baseline and Target Architectures. For AIIMS, these transitions must **accommodate operational continuity**, **minimize disruption**, and **leverage existing investments**, while progressively delivering value in alignment with the Target Architecture.

11.1 Phased Application Rollout Strategy

Transformation is sequenced in three distinct rollout phases, with each phase introducing new capabilities, integrations, and infrastructure in alignment with defined priorities and stakeholder readiness.

11.1.1 Phase 1: Foundation Layer – "Connect & Digitize" (Months 1–6)

Objective: Establish basic digital scaffolding for core hospital services and enable pilot implementations.

Component	Details
Unified Registration System	Digital patient registration with MPI & ABHA integration
Appointment Scheduling Engine	Role-aware, specialty-linked module with triage support
Lab/RIS Integration Layer	HL7 v2-based interfaces to connect lab, imaging, and diagnostic tools
Consent Manager MVP	Initial digital consent workflow for e-consultation & lab reports
API Gateway Deployment	Basic gateway to standardize external/internal API interactions
Training & Change Management	Onboarding modules for clerical staff, nursing, and front-desk teams

Outcome: Paper-to-digital transition in core areas (registration, appointments, labs), aligned with NDHM compliance.

11.1.2 Phase 2: Clinical Systems Enablement – "Unify & Automate" (Months 7–15)

Objective: Expand core capabilities to clinical modules, enhance interoperability, and automate workflows.

Component	Details
Electronic Health Record (EHR)	Department-wide deployment with longitudinal patient view
Mobile/Web Patient Portal	Report downloads, appointment tracking, consent review
Pharmacy Management System	Inventory tracking, prescriptions, dispensing & integration with EHR
Smart Ward System (Pilot)	Real-time vitals monitoring and alerts in 1–2 high-traffic wards
Role-Based Access Control	Central IAM + RBAC for clinicians, students, admin

FHIR Transformation Layer	FHIR resource creation for clinical encounters, labs, medications
Interfacing with NDHM HIE-CM	Federated data exchange with consent for remote access

Outcome: Integrated digital workflows for outpatient, inpatient, and pharmacy operations with patient access layers.

11.1.3 Phase 3: Intelligence & Optimization – "Scale & Predict" (Months 16–24)

Objective: Build analytical capabilities, extend interoperability across national systems, and deploy smart automation.

Component	Details
Healthcare Data Lake	Real-time ingestion of structured/unstructured records for analytics
AI-Enabled Diagnostic Engine	Rule-based + ML-based diagnostic support in radiology and triage
Hospital Command Center	Live dashboards for occupancy, turnaround time, asset utilization
Full Smart Ward Rollout	Expand to ICUs, high-dependency units, and maternity wards
Academic & Research Portal	RedCap + EHR-linked research environment with secure access
NDHM Certification	Final validation of interoperability, consent, and federated exchange

Outcome: AIIMS becomes a digitally mature, analytics-powered institution contributing to the national health grid.

11.2 Data Lake & ETL Transition Strategy

To ensure continuity and clean migration of patient and clinical records:

Transition Stage	Key Actions
Data Staging Environment	Temporary data warehouse for harmonizing legacy system exports
ETL Process Design	Deduplication, patient record matching, and structure validation
Metadata Mapping	Auto-tagging fields to FHIR/LOINC/ICD-11 terminology

Parallel Runs	Run legacy and new systems in parallel for key departments during transition
Quality Assurance	Clinical team validation of migrated records with rollback capability

11.3 Legacy System Coexistence and Support

Given the complex and variable digitization levels across AIIMS departments, legacy systems must coexist during the transition.

Approach to Legacy System Handling:

Component Area	Action Strategy
Radiology (PACS)	Connect to new EHR via HL7 interfaces, phase-out in Year 2
Departmental Lab Tools	Wrap with API adapters for initial integration; retire post Phase 2
Custom Pharmacy Software	Operate in parallel with new ERP until full inventory validation
HR/Finance Modules	Remain standalone; integrated via dashboard APIs in Phase 3

Governance: Each legacy module has an assigned "sunset owner" responsible for timeline tracking and replacement validation.

11.4 Governance and Risk Mitigation Across Transitions

Risk Category	Mitigation Approach
Workflow Disruption	Parallel run with legacy; simulate clinical flows in UAT before go-live
Data Loss or Errors	Multi-step validation, clinical SME approvals, audit logging
Training Gaps	Phased training with role-based LMS content, including language options
Vendor Delays	Buffer windows between phases; milestone-based contracts
Compliance Failures	Continuous internal audit during staging + sandbox NDHM tests

11.5 Visual Transition Architecture Diagrams

1. **Phased Roadmap Timeline (Gantt-style)**
2. **Application Enablement Wave Diagrams**
3. **Legacy-to-Target System Mapping Matrix**
4. **MPI/Data Lake Evolution Diagram**
5. **Department Readiness Scorecard Grid**

12. Architecture Artifacts List

This section outlines the complete set of **architecture deliverables and models** developed as part of Phase C (Information Systems Architecture), covering both Application and Data domains. These artifacts support **communication, validation, governance, and reuse**, and will be referenced throughout Phases D–F for transition, implementation, and change management.

12.1 Application Architecture Artifacts

Artifact Name	Description
Application Landscape Diagram	High-level view of major applications, modules, and their interactions
Application Communication Model	Illustrates data and control flow between components (e.g., EHR ↔ Lab ↔ Pharmacy)
Application Deployment Model	Container-based microservices deployment architecture using Kubernetes
Application Use Case Model	Captures role-specific scenarios (e.g., OPD doctor consult, patient self-check-in)
Functional Component Map	Breakdown of EHR, Telemedicine, Pharmacy, Scheduling, and Academic modules
Interoperability API Map	Visual list of APIs (internal/external) categorized by protocol (REST, HL7, FHIR)
App Lifecycle Diagram	Shows application onboarding, versioning, and deprecation plans
CRUD Matrix	Cross-maps applications with data entities they Create, Read, Update, Delete
Application Gap Analysis Table	Lists missing or underperforming functions against target model

12.2 Data Architecture Artifacts

Artifact Name	Description
Conceptual Data Model	Entity-relationship diagram (ERD) showing core entities like Patient, Encounter, Lab
Logical Data Model (LDM)	Includes attributes, keys, relationships, normalization levels
Physical Data Model (PDM)	Defines table structures, indexes, partitions for storage (PostgreSQL, Hadoop)
Data Flow Diagrams (DFD)	Shows flow of data from source (registration) to destinations (EHR, Data Lake)
Metadata Repository Blueprint	Model for storing data definitions, tags, lineage, and version metadata
Master Patient Index (MPI) Mapping	Shows data elements used to match/deduplicate patients across departments
Data Lifecycle Model	Illustrates create/read/modify/archive stages for each data domain
Consent Flow Diagram	End-to-end view of how patient consent is requested, stored, verified, revoked
Data Classification Matrix	Maps data types (clinical, demographic, financial) to protection levels
HL7/FHIR Mapping Table	Shows equivalence of internal data fields with HL7 v2 and FHIR R4 standards

12.3 Security, Privacy, and Access Artifacts

Artifact Name	Description
IAM/RBAC Matrix	Maps system roles (doctor, nurse, admin, researcher) to permissions
Security Policy Control Matrix	Aligns implemented controls with standards (HIPAA, NDHM, GDPR)
Audit Logging Architecture	Describes log generation, storage, query access, and alerting

Data Protection Blueprint	Shows encryption layers, tokenization, and anonymization flows
Privacy Consent Log Schema	Data schema for capturing consent records, access history, timestamps

12.4 Transition & Migration Artifacts

Artifact Name	Description
Application Transition Plan	Maps current apps to target platforms over transition phases
Data Migration Flow	ETL pipelines, staging layers, QA checkpoints, rollback procedures
Legacy System Coexistence Strategy	Documents integration approach, cut-over timelines, and fallback mechanisms
Capability Deployment Timeline	Gantt-style breakdown of function rollouts over months
UAT/Go-Live Readiness Checklists	Used for clinical validation, dry runs, and go-live assessments

12.5 Supporting Artifacts & Visuals

Artifact Name	Description
Stakeholder Concerns Traceability Matrix	Links architecture decisions to stakeholder priorities from Phase A
Requirements-to-Functionality Matrix	Ensures business needs from Phase B are met by Phase C designs
Architecture Decision Log	Documents design choices, trade-offs, alternatives considered
Tooling and Technology Selection Log	Evaluation notes and justification for chosen platforms/tools
Architecture Heat Maps	Color-coded views showing maturity and capability coverage per module

12.6 Artifact Standards and Formats

Type	Tools/Standards Used
Diagrams	ArchiMate, BPMN 2.0, Draw.io, Lucidchart
Data Models	ERD tools (MySQL Workbench, dbdiagram.io), JSON/XML Schemas
Documents	TOGAF ADM templates, Word/PDF, Confluence pages
Repositories	GitHub/Bitbucket for version control; centralized EA wiki
Meta-tags	ISO 11179 for data element metadata; Dublin Core for documentation

12.7 Governance and Reusability of Artifacts

- **All artifacts are stored** in the AIIMS Enterprise Architecture Repository (cloud-hosted, access-controlled).
- **Versioning controlled** through Git workflows and aligned with TOGAF ADM phase checkpoints.
- **Reusable elements** (e.g., Consent Flow, HL7 mappings, MPI logic) are tagged as baseline assets for reuse in other public health deployments (e.g., Safdarjung, RML).

13. Mapping to Architecture Repository

The Architecture Repository provides a **centralized, structured, and version-controlled environment** to store all architecture-related artifacts, ensuring traceability, reuse, compliance, and knowledge continuity across the enterprise lifecycle.

In the AIIMS context, the repository is a critical tool to support the **progressive digital transformation**, enabling collaboration among clinical, technical, academic, and governance teams.

13.1 Reference Models Used

A number of foundational models were adapted or extended to guide the architecture development process:

Reference Model	Application

TOGAF Foundation Architecture	Baseline repository structure, ADM phase mapping
OpenHIE Reference Model	Interoperability, health information exchange, open standards adoption
OpenEHR Archetype Model	Clinical record structuring, reusability, and semantic consistency
NDHM / ABDM Reference Stack	India-specific digital health standards and compliance frameworks
NIST Cybersecurity Framework	Guiding principles for security controls, auditing, and breach response

13.2 Standards and Templates Followed

The repository enforces the use of standardized templates, naming conventions, and modeling approaches to ensure consistency and facilitate ease of navigation.

Artifact Type	Standard / Template Used
Data Models (ERDs, DFDs)	UML, ISO 11179, ArchiMate, dbdiagram.io
API Specifications	OpenAPI (Swagger) with FHIR JSON schema annotations
Architecture Diagrams	ArchiMate 3.1, BPMN 2.0 for process flows
Policy Documents	NDHM Compliance Template, AIIMS-specific security checklists
Capability Maps & Matrices	TOGAF metamodel-based spreadsheets and visual maps
Logging & Consent Schemas	JSON-LD, HL7 CDA, NDHM Consent Artifact format

13.3 Structure of the Architecture Repository

The repository is organized into modular directories corresponding to TOGAF content framework domains and layers.

Core Repository Domains:

Domain	Contents
Architecture Metamodel	Taxonomy of building blocks, capability definitions, and architecture types

Architecture Landscape	Baseline, Transition, and Target Architecture snapshots
Solutions Repository	Evaluated SBBs, vendor mappings, Open Source stacks (OpenMRS, Kafka, etc.)
Governance Repository	Logs, decision registers, approval workflows, review meeting notes
Standards & Compliance	HL7, FHIR, ICD-11 mappings, NDHM sandbox specs, policy docs
Project Portfolio	Implementation initiatives, phase-wise rollout plans, KPI dashboards
Stakeholder Views	Persona documents, concern-resolution mapping, change management assets

13.4 Version Control and Change Management

To ensure traceability, the repository integrates version control workflows for all key artifacts:

- **Git-based versioning (GitHub/GitLab/Bitbucket)** used for all documents, diagrams, code, and configurations.
- **Branching structure** aligns with TOGAF phases (e.g., phase-c-dev, phase-c-final, phase-d-prep).
- **Change logs** capture the rationale, author, stakeholder approvals, and impact for every update.
- **Automated diff tracking** is enabled for JSON/XML artifacts (FHIR resources, consent logs, etc.)

13.5 Artifact Reuse Strategy

The architecture repository is designed to support reuse within AIIMS and other healthcare institutions across India:

Reusable Element	Application Context
HL7/FHIR API Blueprints	Can be adopted by other NDHM-compliant hospitals
Consent Flow Logic & UI	Modular React component usable in other state-run digital health apps
Smart Ward Alerting Logic	IoT architecture pattern sharable with trauma and emergency hospitals
Master Data Models (MPI, Encounter)	Based on OpenEHR; portable across tertiary care networks
ETL Pipelines	Parameterized workflows usable by labs and radiology units

Each reusable component is tagged with metadata (e.g., creator, domain, date, dependencies) and stored under "Shared Building Blocks."

13.6 Repository Hosting and Access

Hosting Model	Details
Repository Platform	Cloud-hosted (AWS S3 + GitHub/GitLab + secure web portal access)
User Roles	Architect, Reviewer, Clinical Lead, Developer, Compliance Officer
Access Controls	Role-based access with MFA + audit trails for downloads/edits
Backup Strategy	Nightly encrypted backups with 30-day version retention
Search & Indexing	Tag-based metadata search, full-text indexing of uploaded artifacts

13.7 Compliance and Review Integration

- Repository integrated with **architecture review cycles** (monthly)
- All updates undergo **review sign-off** by EA governance board at AIIMS
- Provides evidence base for **NABH audits, NDHM sandbox submissions, and funding reviews**

13.8 Future Enhancements (Planned)

- Integration with **EA tools** (e.g., Archi, Avolution ABACUS, Sparx EA) for direct model export
- Support for **linked data** (RDF/OWL) to semantically connect datasets across hospitals
- Embed **automated artifact completeness checklists** before finalization and board submission

This repository strategy ensures that the architecture work is **future-proof, shareable, and continuously improvable**, enabling AIIMS to lead not just in care delivery, but also in architecture maturity and innovation stewardship.