Software Requirements Specification (SRS) for Healthcare Data Management System (HDMS)

1. Introduction

The **Healthcare Data Management System (HDMS)** is designed to **securely manage** patient records, audit logs, compliance reports, and role-based access control while ensuring **data integrity, privacy, and regulatory compliance**. This document outlines the **functional, non-functional, and technical requirements** for HDMS.

1.2 Document Conventions

This document follows the **IEEE 830-1998** standard for Software Requirements Specification (SRS).

1.3 Intended Audience and Reading Suggestions

This document is intended for:

- **Business Analysts** – To ensure alignment with business goals.
- **Developers** – To understand system architecture and features.
- **Testers** – To validate system functionality.
- **Project Managers** – To track development progress.

1.4 Product Scope

HDMS is a **web-based system** that enables healthcare institutions to:

- Securely **store, retrieve, and manage** patient records.
- Maintain **regulatory compliance (HIPAA, GDPR, ISO 27001)**.
- Provide **role-based access control (RBAC)** to different user types.
- Generate **audit logs and compliance reports**.
- Ensure **data encryption and security** through industry-standard mechanisms.

1.5 References

- **HIPAA (Health Insurance Portability and Accountability Act)**
- **GDPR (General Data Protection Regulation)**
- **ISO 27001 (Information Security Management)**
- **IEEE 830-1998 SRS Standard**

2. System Architecture & Technology Stack

2.1 System Architecture

The **HDMS** follows a **three-tier architecture** to ensure scalability, security, and maintainability:

- **Presentation Layer**: Web-based UI for data access and management.
- **Application Layer**: RESTful APIs and microservices that handle business logic.
- **Data Layer**:

- **Relational database (PostgreSQL)** for structured healthcare data.
- **NoSQL database (MongoDB)** for unstructured data such as logs and documents.

2.2 Technology Stack

Component	Technology
Frontend	React.js, TypeScript, Material UI
Backend	Node.js, Express.js
Database	PostgreSQL (Relational), MongoDB (Unstructured Data)
Authentication	OAuth 2.0, JWT, Multi-Factor Authentication (MFA)
Security	TLS 1.3, AES-256 Encryption, Role-Based Access Control (RBAC)
APIs	RESTful APIs with Swagger documentation
CI/CD Pipeline	GitHub Actions, Docker, Kubernetes
Testing Tools	Xray (Test Management), Jira (Bug Tracking), Postman (API Testing)
Cloud Deployment	AWS (EC2, S3, RDS, Lambda)
Logging & Monitoring	ELK Stack (Elasticsearch, Logstash, Kibana), Prometheus

3. Overall Description

3.1 Product Perspective

The **Healthcare Data Management System (HDMS)** is a **centralized platform** that integrates with various healthcare providers and institutions. It provides a **secure, efficient, and scalable** way to manage patient data while ensuring **compliance with healthcare regulations**.

3.2 Product Features

The system includes the following **key features**:

1. User Management
- Secure **authentication using OAuth 2.0, JWT, and MFA**.
- **Role-Based Access Control (RBAC)** for different user levels (Admin, Doctor, Nurse, Receptionist, etc.).
- Password recovery and security mechanisms.

2. Patient Records Management
- CRUD operations (Create, Read, Update, Delete) for patient records.
- **Access control policies** for sensitive patient data.
- Integration with **Electronic Health Records (EHR)**.

3. Audit Logging & Compliance Reporting
- **Automated logging** of user actions for security tracking.
- **Generate compliance reports** for HIPAA, GDPR, and ISO 27001 audits.
- Prevent unauthorized modifications of logs.

4. API Integration & Interoperability
- RESTful APIs documented with **Swagger**.

- Integration with **third-party healthcare applications**.
- Secure API access using **OAuth 2.0 authentication**.

5. Security & Data Protection

- **TLS 1.3 encryption** for secure data transmission.
- **AES-256 encryption** for sensitive patient data storage.
- **Intrusion detection & session timeout mechanisms**.

6. Logging & Monitoring

- **Real-time system monitoring** using ELK Stack.
- **Alert mechanisms** for security breaches.
- **Automated backup & disaster recovery**.

3.3 User Characteristics

User Role	Description
Admin	Manages user roles, permissions, and system settings.
Doctor	Accesses and updates patient records.
Nurse	Assists doctors and updates patient health data.
Receptionist	Manages appointments and patient registration.
Compliance Officer	Generates audit reports and ensures compliance.

3.4 Constraints

- The system **must comply** with **HIPAA, GDPR, and ISO 27001**.
- Must support at least **100,000 concurrent users**.
- API response time should be **less than 200ms**.

4. Specific Requirements

4.1 Functional Requirements

ID	Requirement	Description
FR-001	User Authentication	Users must log in using **OAuth 2.0 and MFA**.
FR-002	Role-Based Access	Different user roles must have different access levels.
FR-003	Patient Record Management	Users with proper permissions should be able to create, update, and delete records.
FR-004	Audit Logging	All system activities should be logged for security and compliance tracking.
FR-005	Compliance Reporting	Generate reports based on audit logs.
FR-006	Data Encryption	Store and transmit sensitive data using **AES-256 & TLS 1.3**.

4.2 Non-Functional Requirements

ID	Requirement	Description
NFR-001	Security	Data must be **encrypted** and **securely transmitted**.
NFR-002	Performance	API response time **< 200ms**.
NFR-003	Availability	System must maintain **99.99% uptime**.

NFR-004	Scalability	Must support **100,000+ concurrent users**.
NFR-005	Compliance	Must meet **HIPAA, GDPR, and ISO 27001** standards.

5. External Interface Requirements

- **User Interfaces**: Web-based UI with React.js.
- **Hardware Interfaces**: Cloud-based deployment on AWS.
- **Software Interfaces**: RESTful API with Swagger documentation.
- **Communication Interfaces**: Secure HTTPS with TLS 1.3.

6. System Maintenance & Compliance

- **Regular security patches and updates**.
- **Automated backup & disaster recovery plans**.
- **Annual compliance audits** for HIPAA & GDPR

Application Features to be Tested

1. **User Authentication & Role-Based Access Control** (Login, MFA, Role Assignments)
2. **Data Collection & Storage** (Structured & Unstructured Data Entry)
3. **Audit Management & Compliance Reports**
4. **API Integration with External Hospital Systems**
5. **System Performance & Security Controls**