### **Software Requirements Specification (SRS) for Electronic Health Record (EHR) Management System**

#### **1. Introduction**

1.1 **Purpose**This SRS outlines the functionalities and specifications of the "Electronic Health Record (EHR) Management System" (EHRMS). The system is designed to be a secure, cloud-based solution for healthcare institutions to manage, store, and retrieve patient records efficiently.

1.2 **Scope**The EHRMS allows hospitals and clinics to handle all patient-related data, including health records, medications, appointments, and billing. It supports healthcare professionals like doctors, nurses, and administrative staff through role-based access, ensuring secure management of sensitive medical information.

1.3 **Definitions, Acronyms, and Abbreviations**

* **EHR**: Electronic Health Record
* **HIPAA**: Health Insurance Portability and Accountability Act
* **SRS**: Software Requirements Specificatio

1.4 **References**

* HIPAA guidelines for healthcare data security
* National Institute of Standards and Technology (NIST) for cloud computing standards

1.5 **Overview**The document describes the system’s functional and non-functional requirements, database design, security protocols, and user interface specifications.

#### **2. Overall Description**

2.1 **System Environment**The EHRMS will be deployed in a cloud-based environment to ensure data availability, accessibility, and security. It will be accessible via web browsers on both desktop and mobile devices.

2.2 **Product Functions**

* **Patient Management**: Record and manage patient information, including medical history, allergies, and demographics.
* **Appointment Scheduling**: Manage appointments between patients and healthcare professionals.
* **Electronic Health Records**: Store, edit, and retrieve patient records such as diagnosis, treatment history, lab results, and prescriptions.
* **Billing and Insurance**: Manage patient billing information and insurance details.
* **Audit and Compliance**: Track user activities for HIPAA compliance through an audit trail.

2.3 **User Classes and Characteristics**

* **Administrator**: Manages user roles, system configurations, and permissions.
* **Doctor/Nurse**: Views and manages patient records, prescriptions, and lab results.
* **Receptionist**: Handles patient registration, appointment scheduling, and billing.
* **Patient**: Optionally, through a patient portal, patients can access their records, request prescriptions, and view appointments.

2.4 **Operating Environment**

* The system will run on modern web browsers (Chrome, Firefox, Safari).
* Mobile responsiveness is required for healthcare professionals on the move.

2.5 **Design and Implementation Constraints**

* The system must comply with HIPAA and other medical data protection regulations.
* Encryption must be used for all sensitive data.
* Performance must meet healthcare standards for quick data retrieval and reliability.

2.6 **Assumptions and Dependencies**

* Internet access is required for real-time access to cloud-based data.
* Integration with external systems like lab testing services may require additional APIs.

#### **3. Specific Requirements**

3.1 **Functional Requirements**

1. **User Login**
   * Secure login using email and password.
   * Two-factor authentication for increased security.
2. **Patient Registration**
   * Input fields for patient personal details, contact information, medical history, and allergies.
   * Validation for email, phone number, and date of birth.
3. **Health Record Management**
   * CRUD (Create, Read, Update, Delete) operations for patient medical records.
   * Upload and manage attachments (e.g., scans, reports).
4. **Appointment Scheduling**
   * Create, edit, and cancel appointments with automatic notifications for patients and healthcare providers.
   * Display upcoming and past appointments.
5. **Medication Management**
   * Add, edit, and view prescribed medications for each patient, including dosage and frequency.
   * Manage medication refills and prescriptions.
6. **Billing**
   * Generate invoices for patient services, including consultations, lab tests, and prescriptions.
   * Track payment status (paid, pending, canceled).
7. **Insurance**
   * Store and manage patient insurance details and claims.
   * Validate expiration dates of policies.
8. **Audit Trail**
   * Log user activities (record updates, logins, billing) for compliance.
9. **Reporting**
   * Generate customizable reports based on patient records, billing, or appointments.

3.2 **Non-Functional Requirements**

1. **Performance**
   * System response time should not exceed 2 seconds for database queries and record retrievals.
2. **Security**
   * Role-based access control to ensure data is accessed only by authorized users.
   * End-to-end encryption of patient records and sensitive information.
   * Regular security audits and compliance checks.
3. **Scalability**
   * The system should be able to handle a growing number of users and records without performance degradation.
4. **Usability**
   * Intuitive and user-friendly interface designed for healthcare professionals.
5. **Availability**
   * 99.9% uptime with minimal disruptions for maintenance.

#### **4. Database Design**

4.1 **Database Tables** The database design includes key tables for managing users, patients, appointments, medications, and billing. Each table is designed with foreign key relationships to ensure data integrity.

* **Users**Stores details of system users (doctors, nurses, admins) and their roles.
* **Patients**Stores patient information, including demographics and medical history.
* **EHRRecords**Stores detailed medical records related to each patient.
* **Appointments**Stores scheduled appointments and their statuses (scheduled, completed, canceled).
* **Medications**Stores prescribed medications with dosage and frequency information.
* **Billing**Stores patient billing records, payment status, and methods.
* **AuditTrail**Logs user activity for tracking and security.

#### **5. Security and Privacy**

5.1 **Security Requirements**

* All patient records and sensitive data must be encrypted using industry-standard protocols (e.g., AES-256).
* User passwords should be stored using a secure hash (e.g., SHA-256).
* Implement regular backups and disaster recovery plans.

5.2 **Compliance**The system must adhere to all regulatory frameworks like HIPAA, ensuring the confidentiality and integrity of health records.

#### **6. User Interface Requirements**

* **Login Page**: Simple interface for secure user authentication.
* **Dashboard**: A centralized interface displaying key metrics and quick access to functionalities.
* **Patient Profile Page**: A detailed view of patient demographics and medical history.
* **EHR Management Page**: Forms to view, edit, and manage patient records.
* **Appointment Scheduling Page**: A calendar interface for managing appointments.

#### **7. Appendices**

7.1 **Glossary**

* **EHR**: Electronic Health Record.
* **CRUD**: Create, Read, Update, Delete.

7.2 **References**

* HIPAA Guidelines for Data Security.
* NIST Standards for Cloud Computing.