Software Requirement Document

Session 2021-2025

Submitted by:

Yahya Mirza 2021-CS-11

M. Uzair 2021-CS-17

Haider Sultan 2021-CS-85

M. Abdullah 2021-CS-104

Ammad Bin Shahid 2021-CS-154

Submitted to:

Dr Muhammad Shoib

Department of Computer Science

University of Engineering and Technology, Lahore

Pakistan

Contents

1 Introduction

1.1 Purpose

The purpose of this SRS document is to define the requirements for the Telemedicine Web Application. This system is designed to facilitate remote healthcare consultations, diagnostics, and follow-ups. It will enable healthcare providers to offer virtual consultations, reducing the need for physical hospital visits and improving access to medical care, particularly for patients in rural or underserved areas. This document serves as a guideline for developers, stakeholders, and the healthcare institutions that will utilize the platform.

1.2 Scope

The Telemedicine Web Application will provide a secure, scalable, and accessible platform for healthcare services. It will include features for patient registration, appointment scheduling, virtual consultations, medical records management, and secure prescription services. The application will support AI-powered diagnostic tools, enabling physicians to make informed decisions. A focus on user-friendly design will cater to both technical and non-technical users, ensuring accessibility across various demographics.

1.3 Definitions, Acronyms, and Abbreviations

- **HIPAA**: Health Insurance Portability and Accountability Act.
- **GDPR**: General Data Protection Regulation.
- **EHR**: Electronic Health Records.
- **AI**: Artificial Intelligence.
- **UI**: User Interface.

1.4 References

- Healthcare Data Protection Guidelines (HIPAA, GDPR).
- Web Accessibility Guidelines (WCAG 2.1).
- FHIR Standards for healthcare interoperability.
- Various standards for AI applications in healthcare.

1.5 Overview

This document provides a comprehensive description of the Telemedicine Web Application's requirements, capturing both functional and non-functional aspects of the system. The primary goal is to support a scalable, secure, and efficient virtual healthcare platform that facilitates real-time interactions between patients and healthcare providers. This overview includes a breakdown of user requirements, system architecture, and compliance standards.

2 Overall Description

2.1 Product Perspective

The Telemedicine Web Application will be a cloud-based system, accessible via web and mobile platforms. It will interface with Electronic Health Records (EHR) systems for seamless patient data access, enabling healthcare providers to view medical histories and manage patient care more effectively. The application will also integrate with third-party services for payment processing, AI diagnostic tools, and secure video communication channels.

2.2 Product Functions

The main functionalities are as follows:

- **Patient Registration and Profile Management**: Allows patients to register, create profiles, and update personal information.
- **Appointment Scheduling and Management**: Patients can schedule, reschedule, or cancel appointments. Notifications and reminders will be sent to both patients and providers.
- **Virtual Consultations**: Enables video, audio, and text-based consultations, allowing providers to diagnose and treat patients remotely.
- **EHR Access**: Healthcare providers can access and update patient records, streamlining patient history review during consultations.
- **Prescription Services**: Providers can generate and send digital prescriptions to pharmacies and patients.

2.3 User Classes and Characteristics

- **Patients**: Typically non-technical users seeking easy and accessible healthcare solutions.
- **Healthcare Providers**: Physicians and other licensed healthcare professionals who deliver care via the platform.
- **Administrative Staff**: System administrators managing appointments, payments, and compliance-related tasks.

2.4 Operating Environment

The system will operate on both web and mobile platforms, with servers hosted on a cloud infrastructure, ensuring scalability, reliability, and ease of maintenance. The system must support common browsers and mobile operating systems (iOS, Android).

2.5 General Constraints

- Adherence to privacy laws (HIPAA, GDPR) is mandatory.
- Support for real-time communication for virtual consultations.
- Bandwidth limitations may impact video call quality.

2.6 Assumptions and Dependencies

- Patients and providers must have stable internet access.
- Reliable integration with third-party APIs for EHR systems, video conferencing, and payment processing.
- Dependence on cloud infrastructure for high availability.

2.7 Functional Requirements

2.7.1 User Registration

Introduction User registration allows patients and healthcare providers to create accounts in the system, enabling access to the platform's services.

Inputs

- Personal information including name, contact details, and date of birth.
- Email address and password for account creation.
- Additional details for healthcare providers such as professional license information and qualifications.

Processing

- Validation of input data for format and completeness.
- Verification of email through a confirmation link.
- Authentication of healthcare provider credentials with licensing databases.

Output

- Confirmation notification of successful registration.
- Access to user dashboard upon login.

2.7.2 Appointment Scheduling

Introduction Appointment scheduling enables patients to book consultations with healthcare providers at their convenience.

Inputs

- Patient's preferred date and time for appointment.
- Type of consultation (video, audio, or text).
- Medical concern or reason for consultation.

Processing

- Check for available slots with chosen healthcare provider.
- Notify provider of the booking request.
- Store appointment details in the database.

Output

- Confirmation of appointment with details of time, date, and consultation link.
- Appointment reminder notification to both patient and provider.

2.7.3 Virtual Consultations

Introduction Virtual consultations provide a platform for real-time interaction between patients and healthcare providers via video, audio, or chat.

Inputs

- Patient's health information and reason for consultation.
- Patient and provider access to audio/video capabilities on their devices.

Processing

- Establish a secure, encrypted connection for audio/video communication.
- Provide an interface for chat and file exchange (e.g., sharing test reports).
- Allow providers to access and view patient health records as needed.

Output

- Real-time consultation experience with secure communication.
- Summary of consultation provided to patient after the session.

2.7.4 Electronic Health Records (EHR) Access

Introduction EHR access allows healthcare providers to view patient records, facilitating informed decision-making during consultations.

Inputs

- Patient health history, diagnostic reports, and medications.
- EHR integration credentials for access to external systems.

Processing

- Retrieve and display relevant patient records to healthcare providers.
- Ensure data is accessible in a readable, user-friendly format.
- Log access events for compliance and security.

Output

- Display of complete medical history and relevant data to the provider.
- Updated EHR with any new consultation notes or diagnoses.

2.7.5 Prescription Generation

Introduction Prescription generation enables healthcare providers to prescribe medications securely and send them to patients.

Inputs

- Diagnosis and treatment plan provided by healthcare provider.
- List of medications and dosage details.

Processing

- Verification of prescribed medications against known drug interactions.
- Generation of a digital prescription document.
- Option for the provider to send prescription to patient's preferred pharmacy.

Output

- Digital prescription document accessible to the patient.
- Prescription record stored in patient's health records for future reference.

2.7.6 Patient Profile Management

Introduction Patient profile management allows patients to view and edit their personal information, health history, and preferences.

Inputs

- Personal information such as name, contact details, and medical history.
- User preferences, such as notification settings and preferred consultation types.

Processing

- Validation and storage of updated profile information.
- Access control to prevent unauthorized modifications.

Output

- Updated profile details available in patient dashboard.
- Notification of successful profile update.

2.7.7 Healthcare Provider Profile Management

Introduction Provider profile management allows healthcare providers to update their professional information and manage consultation schedules.

Inputs

- Professional details such as qualifications, license numbers, and specialty areas.
- Availability schedule and consultation preferences.

Processing

- Validation and storage of professional credentials.
- Update of provider's availability for patient scheduling.

Output

- Updated provider profile displayed to patients.
- Confirmation of schedule updates.

2.7.8 Payment Processing

Introduction Payment processing enables patients to pay for consultations and other services securely through the platform.

Inputs

- Payment details such as credit card information or bank account.
- Invoice or billing information generated for the consultation.

Processing

- Securely handle payment information with PCI-DSS compliance.
- Generate receipts and update payment status for the appointment.

Output

- Payment confirmation and receipt.
- Updated appointment status indicating successful payment.

2.7.9 Notifications and Reminders

Introduction The notification system alerts patients and providers about appointments, updates, and reminders.

Inputs

- Scheduled appointments and user preferences for notifications.
- Important system updates or changes in consultation schedules.

Processing

- Generate reminders and notifications based on user preferences.
- Send alerts via email, SMS, or in-app notifications.

Output

- Timely reminders and alerts for both patients and providers.
- Notification history accessible within user accounts.

2.8 External Interface Requirements

2.8.1 User Interface

- User-friendly, responsive design for both patients and providers.
- Customizable dashboards displaying patient profiles, schedules, and health records.

2.8.2 Hardware Interface

The application will operate on minimal hardware: any device with internet capability such as smartphones, tablets, or desktop computers.

2.8.3 Software Interface

- Integration with third-party Electronic Health Records (EHR) systems.
- APIs for secure video calling and payment processing.

2.8.4 Communication Interface

- Secure, encrypted connections for all communications, particularly for sensitive data.
- Use of Transport Layer Security (TLS) for real-time communication.

2.9 Performance Requirements

- The system must handle high volumes of simultaneous virtual consultations.
- Response times should be under two seconds for most user actions.
- Video consultations should have minimal lag and high-quality video and audio.

2.10 Design Constraints

- **Compliance with Regulations**: Ensure adherence to HIPAA and GDPR standards.
- **Data Encryption**: All sensitive information, especially health records, must be encrypted.

2.11 Attributes

2.11.1 Security

- End-to-end encryption of patient data.
- Multi-factor authentication for accessing sensitive data.

2.11.2 Maintainability

- Regular updates and modular architecture for ease of maintenance.
- Comprehensive documentation for development, deployment, and troubleshooting.

2.12 Other Requirements

- Training and support resources for new users.
- Accessible user guides and troubleshooting documentation.

3 Compliance Requirements

Compliance with regulatory standards is critical to ensure the Telemedicine Web Application protects user data, maintains patient confidentiality, and operates within legal frameworks. The application will adhere to the following requirements:

- **General Data Protection Regulation (GDPR)**: The system will follow GDPR guidelines to ensure that all patient data, especially for users in the European Union, is handled securely and privately. This includes features such as data minimization, access control, and encryption of sensitive information. Additionally, patients will have the right to request access to their data or request its deletion in accordance with GDPR requirements.

- **Health Insurance Portability and Accountability Act (HIPAA)**: For U.S.-based users, the system will comply with HIPAA standards to protect the privacy and security of health information. This includes safeguards like encryption, secure user authentication, and audit trails to track access and changes to patient records. The system will also ensure secure transmission of protected health information (PHI) during video consultations and data exchanges with EHR systems.

- **Web Content Accessibility Guidelines (WCAG 2.1)**: The application will adhere to WCAG 2.1 to ensure accessibility for all users, including those with disabilities. Features will include alternative text for images, keyboard navigation, and compatibility with screen readers. The goal is to make the application accessible to users with visual, auditory, and motor impairments.

- **FHIR Standards for Interoperability**: The system will use the Fast Healthcare Interoperability Resources (FHIR) standard to communicate with other healthcare systems. This ensures seamless data exchange and integration with various EHR systems, enabling providers to access and share patient information efficiently and securely.

- **Data Localization and Retention Policies**: The application will adhere to data localization laws as per regional requirements, storing data in servers located within specific geographic regions when required. Additionally, it will follow retention policies by securely deleting or archiving data after a designated period to comply with local data governance laws.

- **Periodic Compliance Audits**: Regular audits will be conducted to ensure the application remains compliant with HIPAA, GDPR, and other relevant regulations. These audits will include evaluating security protocols, data access logs, and adherence to privacy policies, providing assurance to users that their data is handled responsibly.

- **User Consent and Privacy Policy Compliance**: The application will provide clear information to users regarding how their data will be used. Before collecting or processing any sensitive data, user consent will be obtained through a transparent process that complies with GDPR and HIPAA guidelines.