### Requirements Specification

for Project 1

ITIS 6120

[Requirements Specification](#_ugk3xmkw8djf)

[1. Introduction](#_axzpakiwv67w)

[2. General Requirements](#_doh4ptnjpqr)

[3. Data Requirements](#_6zodvjdg9qu)

[3.1 Patient Information](#_adapvur6uvxd)

[3.2 Appointments](#_4mm8xidqj35j)

[3.3 Medical Records](#_negfxey48kix)

[3.4 Prescriptions](#_i7qwckpb4v3d)

[3.5 Billing](#_bztnmfu9hdtd)

[3.6 Reporting](#_mout01dn7wgm)

[4. Database Design](#_8upvh0k5s0c8)

[4.1 Entity-Relationship Model](#_hsfmn8me80cd)

[4.2 Schema Design](#_2q0fkm5ddrdm)

[4.3 Data Types](#_8ifyrl7xhrhm)

[5. Performance and Scalability](#_lijvyi9snrmy)

[6. Backup and Recovery](#_91geruflpghx)

[7. Compliance and Privacy](#_5ssx1pqrszt4)

### 1. Introduction

* Purpose: The purpose of this document is to specify the database requirements for an ophthalmology practice software system to ensure efficient patient management, appointment scheduling, record-keeping, and billing.
* Scope: The database will support functionalities such as patient registration, appointment scheduling, medical records management, prescription handling, billing, and reporting.

### 2. General Requirements

* Database Management System (DBMS): The system should use a robust and scalable DBMS that supports complex queries, transactions, and high availability.
* Data Integrity and Consistency: Ensure data integrity through referential integrity constraints, unique constraints, and check constraints.
* Security: Implement role-based access controls and ensure that sensitive data, especially patient information, is encrypted.

### 3. Data Requirements

#### 3.1 Patient Information

* Patient Profile: Store comprehensive details, including name, date of birth, contact information, gender, and insurance details.
* Medical History: Record medical history, including previous diagnoses, treatments, allergies, and family medical history.

#### 3.2 Appointments

* Appointment Details: Store appointment dates, times, attending physician, and appointment status (scheduled, completed, canceled).
* Reminders: Mechanism to track and send appointment reminders.

#### 3.3 Medical Records

* Visit Records: Document each patient visit, including date, reason for visit, diagnosis, treatment plan, and follow-up instructions.
* Vision Tests: Detailed records of vision tests conducted, including test type, date, and results.

#### 3.4 Prescriptions

* Prescription Records: Information on prescriptions issued, including medication name, dosage, frequency, and instructions.

#### 3.5 Billing

* Billing Records: Detailed billing information for services rendered, including itemized services, amounts, patient payments, and insurance claims.
* Insurance Information: Store insurance provider details and manage insurance claims processing.

#### 3.6 Reporting

* Report Generation: Support for generating customizable reports for clinical, operational, and financial analysis.

### 4. Database Design

#### 4.1 Entity-Relationship Model

* Entities: Define entities such as Patients, Appointments, MedicalRecords, Prescriptions, Billing, and InsuranceClaims, along with their attributes.
* Relationships: Specify the relationships between entities, including one-to-many and many-to-many relationships, as appropriate.

#### 4.2 Schema Design

* Provide detailed schema designs for each entity, including primary keys, foreign keys, and indexes to optimize query performance.

#### 4.3 Data Types

* Specify appropriate data types for each attribute to ensure data accuracy and efficiency.

### 5. Performance and Scalability

* Indexing: Use indexes strategically to speed up query performance without significantly affecting insert/update performance.
* Scalability: Design the database to be scalable, allowing for easy expansion as the practice grows in size and complexity.

### 6. Backup and Recovery

* Backup Strategy: Implement regular backup procedures to prevent data loss.
* Disaster Recovery: Outline a disaster recovery plan to restore database functionality in case of an outage or data corruption.

### 7. Compliance and Privacy

* Regulatory Compliance: Ensure the database system complies with healthcare regulations, such as HIPAA, for protecting patient privacy and data security.
* Audit Trails: Maintain audit trails of access to sensitive data and changes within the database.