Security and Privacy Requirements

REQ-001: Secure Data Storage and Transmission

- **Description**: All patient data must be encrypted at rest and in transit, ensuring confidentiality and integrity as required by ISO/IEC 27001 and ENS.
- **Acceptance Criteria**:
    - AES-256 encryption for data at rest.
    - TLS 1.2+ encryption for data in transit.
- **Priority**: High
- **Category**: Data Security
- **Applicable Standard**: ISO/IEC 27001:2023【9】, ENS【10】, GDPR Article 32【12】.
- **Justification**: Ensures compliance with international security standards and protects sensitive medical data.

REQ-002: Multi-Factor Authentication (MFA)

- **Description**: Users with administrative and medical roles must authenticate using at least two factors.
- **Acceptance Criteria**:
    - MFA is required for login.
    - Options include OTP via email/SMS or authentication apps.
- **Priority**: High
- **Category**: Access Control
- **Applicable Standard**: ISO/IEC 27001:2023【9】, ENS【10】.
- **Justification**: Prevents unauthorized access and aligns with best security practices.

REQ-003: Role-Based Access Control (RBAC)

- **Description**: System must implement **RBAC** to restrict access to sensitive health information.
- **Acceptance Criteria**:
    - Doctors can access and modify patient records.
    - Administrative staff can only access billing and scheduling data.
    - Patients can only access their own records.

- **Priority**: High
- **Category**: Access Management
- **Applicable Standard**: ENS【10】, GDPR Article 5 (Data Minimization)【12】.
- **Justification**: Limits access to only necessary personnel, reducing security risks.

REQ-004: Audit Logs and Monitoring

- **Description**: The system must log all access, modifications, and data exports.
- **Acceptance Criteria**:
    - Log contains **user ID, timestamp, action performed**.
    - Audit logs are immutable and stored securely for at least 2 years.
- **Priority**: High
- **Category**: Compliance & Monitoring
- **Applicable Standard**: ISO/IEC 27001:2023【9】, ENS【10】, GDPR Article 30【12】.
- **Justification**: Provides traceability for compliance audits.

REQ-005: Data Subject Rights Handling

- **Description**: Patients must be able to access, rectify, delete, and export their personal data.
- **Acceptance Criteria**:
    - User interface to request access and deletion.
    - Automated process to respond within 30 days.
- **Priority**: High
- **Category**: GDPR Compliance
- **Applicable Standard**: GDPR Articles 15-17【12】, LOPDGDD【11】.
- **Justification**: Ensures compliance with GDPR and LOPDGDD for data rights.

Interoperability & Data Integration Requirements

REQ-006: Standardized Data Exchange (FHIR/HL7)

- **Description**: The system must support **FHIR** and **HL7** for interoperability with hospital databases and third-party systems.
- **Acceptance Criteria**:
    - Data export and import in **FHIR JSON/XML** format.

    - API endpoints for data sharing with other healthcare institutions.
- **Priority**: High
- **Category**: Interoperability
- **Applicable Standard**: IEEE 29148【13】.
- **Justification**: Enables easy integration with existing hospital systems.

REQ-007: Electronic Signature Compliance

- **Description**: Medical professionals must be able to **digitally sign** documents within the system.
- **Acceptance Criteria**:
    - Compliance with **eIDAS** for legally recognized digital signatures.
    - Log of signed documents with timestamps.
- **Priority**: High
- **Category**: Legal Compliance
- **Applicable Standard**: ENS【10】.
- **Justification**: Provides legal validity for medical records.

REQ-008: Data Portability

- **Description**: Patients must be able to export their medical history in **structured formats** like XML, JSON, or PDF.
- **Acceptance Criteria**:
    - Export functionality in FHIR format.
    - Option to download as a structured PDF.
- **Priority**: Medium
- **Category**: Interoperability
- **Applicable Standard**: GDPR Article 20【12】.
- **Justification**: Ensures data portability for patient control.

Availability & Disaster Recovery Requirements

REQ-009: High Availability & Redundancy

- **Description**: The system must ensure **99.9% uptime** with redundancy mechanisms.
- **Acceptance Criteria**:

    - Load balancing across multiple servers.
    - Auto-failover in case of server failure.
- **Priority**: High
- **Category**: Reliability
- **Applicable Standard**: ISO/IEC 27001:2023【9】.
- **Justification**: Guarantees system availability for critical healthcare operations.

REQ-010: Automated Backups

- **Description**: The system must have **automated daily backups**, stored securely in a separate location.
- **Acceptance Criteria**:
    - Backups stored for **30 days minimum**.
    - Encrypted and tested for integrity.
- **Priority**: High
- **Category**: Disaster Recovery
- **Applicable Standard**: ENS【10】, ISO/IEC 27001【9】.
- **Justification**: Prevents data loss in case of system failures.