MediCare Electronic Health Record System

Product Requirements Document

Document Version	1.0
Created Date	2025-09-21
Project Key	MED
Project Name	MediCare EHR System
Document Type	Product Requirements Document
Compliance Standards	FDA, IEC 62304, ISO 13485, ISO 27001, GDPR

Table of Contents

1. Executive Summary

The MediCare Electronic Health Record (EHR) System is a comprehensive healthcare software solution designed to meet the complex regulatory requirements of the healthcare industry. This system will provide secure, compliant, and efficient management of patient health records while ensuring adherence to FDA, IEC 62304, ISO 13485, ISO 27001, and GDPR standards. The system addresses critical healthcare challenges including data security, regulatory compliance, clinical decision support, and seamless integration with existing healthcare workflows. Our solution will reduce manual processes, improve patient care quality, and ensure full traceability for regulatory compliance.

2. Product Overview

The MediCare EHR System is a cloud-based electronic health record platform that enables healthcare providers to securely store, manage, and access patient health information. The system provides comprehensive functionality for patient data management, clinical decision support, and regulatory compliance. Key capabilities include: • Secure patient data encryption and storage • Multi-factor authentication and access control • Comprehensive audit trails and logging • Automated backup and recovery systems • Clinical decision support for drug interactions • HL7 FHIR integration for interoperability • GDPR-compliant data privacy controls

3. Business Objectives

1. Improve patient care quality through better data access and clinical decision support
2. Ensure full regulatory compliance with healthcare standards and regulations
3. Reduce administrative burden through automation and streamlined workflows
4. Enhance data security and privacy protection for patient information
5. Enable seamless integration with existing healthcare systems and workflows
6. Provide scalable and maintainable solution for healthcare organizations
7. Achieve cost savings through reduced manual processes and improved efficiency

4. Functional Requirements

4.1 Patient Data Management

The system must provide comprehensive patient data management capabilities including secure storage, encryption, and access control for all patient health information. This includes demographic data, medical history, diagnoses, treatments, medications, and laboratory results.

4.2 Security and Compliance

The system must implement robust security measures including multi-factor authentication, encryption at rest and in transit, comprehensive audit logging, and automated backup systems. All security measures must comply with healthcare industry standards and regulations.

4.3 Clinical Decision Support

The system must provide clinical decision support capabilities including drug interaction checking, clinical guidelines integration, and automated alerts for potential patient safety issues. The system should integrate with external clinical databases and provide real-time decision support.

5. Non-Functional Requirements

Requirement Category	Specification
Performance	System must support 1000+ concurrent users
Availability	99.9% uptime with maximum 8.76 hours downtime per year
Scalability	Support for 100,000+ patient records
Response Time	Page load times under 3 seconds
Data Retention	Minimum 7 years patient data retention
Backup Frequency	Daily automated backups with 30-day retention
Security	AES-256 encryption, TLS 1.3, MFA required
Compliance	FDA, IEC 62304, ISO 13485, ISO 27001, GDPR

6. Compliance Requirements

1. FDA 21 CFR Part 11 - Electronic Records and Signatures
2. IEC 62304 - Medical Device Software Life Cycle Processes
3. ISO 13485 - Medical Devices Quality Management Systems
4. ISO 27001 - Information Security Management Systems
5. GDPR - General Data Protection Regulation
6. HIPAA - Health Insurance Portability and Accountability Act
7. HL7 FHIR R4 - Fast Healthcare Interoperability Resources

7. User Stories and Acceptance Criteria

7.1 Implement Patient Data Encryption

Description: As a healthcare provider, I need patient data to be encrypted so that sensitive information is protected from unauthorized access.

Epic: MED-101

Story Points: 8

Compliance Standards: HIPAA, ISO 27001

Acceptance Criteria:

- All patient data stored in database is encrypted using AES-256
- Data transmission uses TLS 1.3 encryption

- Encryption keys are managed using secure key management system
- Data remains encrypted during backup operations

7.2 Multi-Factor Authentication Implementation

Description: As a system administrator, I need multi-factor authentication to be implemented so that user accounts are protected from unauthorized access.

Epic: MED-101

Story Points: 5

Compliance Standards: HIPAA, ISO 27001, IEC 62304

Acceptance Criteria:

- Users must authenticate with username and password
- Second factor authentication (SMS, email, or authenticator app) is required
- Session timeout occurs after 30 minutes of inactivity
- Failed login attempts are logged and account locked after 5 attempts

7.3 Audit Trail and Logging System

Description: As a compliance officer, I need comprehensive audit logging so that all user actions and data access can be tracked for regulatory compliance.

Epic: MED-101

Story Points: 13

Compliance Standards: FDA, HIPAA, ISO 13485

Acceptance Criteria:

- All user actions are logged with timestamp, user ID, and action details
- Data access events are logged including what data was accessed
- Audit logs are tamper-proof and cannot be modified
- Audit logs are retained for minimum 7 years
- Audit logs can be exported for regulatory review

7.4 Automated Backup and Recovery System

Description: As a system administrator, I need automated backup and recovery capabilities so that patient data is protected and can be restored in case of system failure.

Epic: MED-100

Story Points: 8

Compliance Standards: HIPAA, ISO 13485

Acceptance Criteria:

- Automated daily backups are performed at 2:00 AM
- Backups are stored in geographically separate location
- Backup integrity verification is performed after each backup
- System can be restored from backup within 4 hours
- Point-in-time recovery is available for last 30 days

7.5 Clinical Decision Support for Drug Interactions

Description: As a healthcare provider, I need drug interaction checking so that I can avoid prescribing medications that may interact dangerously with patient's current medications.

Epic: MED-102

Story Points: 13

Compliance Standards: FDA, IEC 62304

Acceptance Criteria:

- Drug interaction checking is performed before medication orders
- Allergy alerts are displayed when prescribing medications
- Clinical guidelines are accessible and contextually relevant
- Decision support alerts are configurable by healthcare providers
- All alerts are logged for quality improvement purposes

7.6 System Performance Optimization

Description: As a healthcare provider, I need the system to respond quickly so that I can efficiently care for patients without delays.

Epic: MED-100

Story Points: 8

Compliance Standards: ISO 13485

Acceptance Criteria:

- 95% of user queries respond within 2 seconds
- System supports 1000 concurrent users without degradation
- Database queries are optimized for sub-second response times
- System availability is 99.9% during business hours

7.7 GDPR Data Privacy Controls

Description: As a patient, I need control over my personal data so that my privacy rights are respected according to GDPR regulations.

Epic: MED-101

Story Points: 13

Compliance Standards: GDPR, HIPAA

Acceptance Criteria:

- Patient consent is obtained before data collection
- Consent can be withdrawn at any time
- Data processing purposes are clearly documented
- Right to data portability is supported
- Right to data erasure is implemented with audit trail

7.8 HL7 FHIR Integration

Description: As a healthcare system administrator, I need HL7 FHIR integration so that the EHR can exchange data with other healthcare systems.

Epic: MED-102

Story Points: 21

Compliance Standards: IEC 62304, ISO 13485

Acceptance Criteria:

- HL7 FHIR R4 standard is supported for data exchange
- DICOM integration is available for medical imaging
- SMART on FHIR apps can be integrated
- Data mapping and transformation tools are provided
- API documentation is available for third-party integrations

8. Technical Architecture

The MediCare EHR System will be built using a modern, cloud-native architecture with the following key components: • **Frontend:** React.js-based web application with responsive design • **Backend API:** Python/Django REST framework with microservices architecture • **Database:** PostgreSQL with encryption at rest and automated backups • **Authentication:** OAuth 2.0 with multi-factor authentication support • **Encryption:** AES-256 for data at rest, TLS 1.3 for data in transit • **Cloud Platform:** Google Cloud Platform with auto-scaling capabilities • **Integration:** HL7 FHIR R4 APIs for healthcare system interoperability • **Monitoring:** Comprehensive logging and monitoring with audit trails

9. Security Requirements

1. Implement AES-256 encryption for all patient data at rest
2. Use TLS 1.3 for all data transmission and API communications
3. Require multi-factor authentication for all user accounts
4. Implement role-based access control with granular permissions
5. Maintain comprehensive audit logs for all system activities
6. Implement automated key rotation and management systems
7. Ensure secure backup and recovery procedures
8. Conduct regular security assessments and penetration testing

10. Performance Requirements

1. Support 1000+ concurrent users without performance degradation
2. Achieve page load times under 3 seconds for 95% of requests
3. Process 10,000+ patient records per hour during peak usage
4. Maintain 99.9% system availability with maximum 8.76 hours downtime per year
5. Support horizontal scaling to accommodate future growth
6. Implement caching strategies for frequently accessed data
7. Optimize database queries for sub-second response times

11. Integration Requirements

1. HL7 FHIR R4 API integration for healthcare system interoperability

2. Support for standard healthcare data formats (HL7, DICOM, etc.)
3. Integration with existing hospital information systems (HIS)
4. Laboratory information system (LIS) integration capabilities
5. Pharmacy management system integration for drug interaction checking
6. Radiology information system (RIS) integration for imaging data
7. Third-party authentication provider integration (Active Directory, LDAP)

12. Risk Assessment

Risk	Impact	Probability	Mitigation Strategy
Data Breach	High	Medium	Implement comprehensive security measures, reg
Regulatory Non-compliance	High	Low	Continuous compliance monitoring, expert consult
System Downtime	Medium	Low	Redundant systems, automated failover
Integration Failures	Medium	Medium	Thorough testing, fallback procedures
Performance Issues	Medium	Low	Load testing, performance monitoring
User Adoption	Medium	Medium	Training programs, user-friendly design

13. Success Metrics

1. Achieve 99.9% system uptime and availability
2. Complete all regulatory compliance audits successfully
3. Reduce patient data access time by 50% compared to legacy systems
4. Achieve 95% user satisfaction rating in post-implementation surveys
5. Process 100% of patient records with full audit trail compliance
6. Complete integration with 100% of required external systems
7. Achieve zero security incidents or data breaches
8. Reduce manual data entry by 75% through automation

14. Implementation Timeline

Phase	Duration	Key Deliverables
Phase 1: Foundation	8 weeks	Core infrastructure, security framework, basic patient data

Phase 2: Security & Compliance	6 weeks	Encryption implementation, audit logging, compliance valid
Phase 3: Clinical Features	10 weeks	Clinical decision support, drug interaction checking
Phase 4: Integration	8 weeks	HL7 FHIR integration, external system connections
Phase 5: Testing & Validation	6 weeks	Comprehensive testing, performance optimization
Phase 6: Deployment	4 weeks	Production deployment, user training, go-live support

Document Version 1.0 | Generated: 2025-09-21 01:04:25