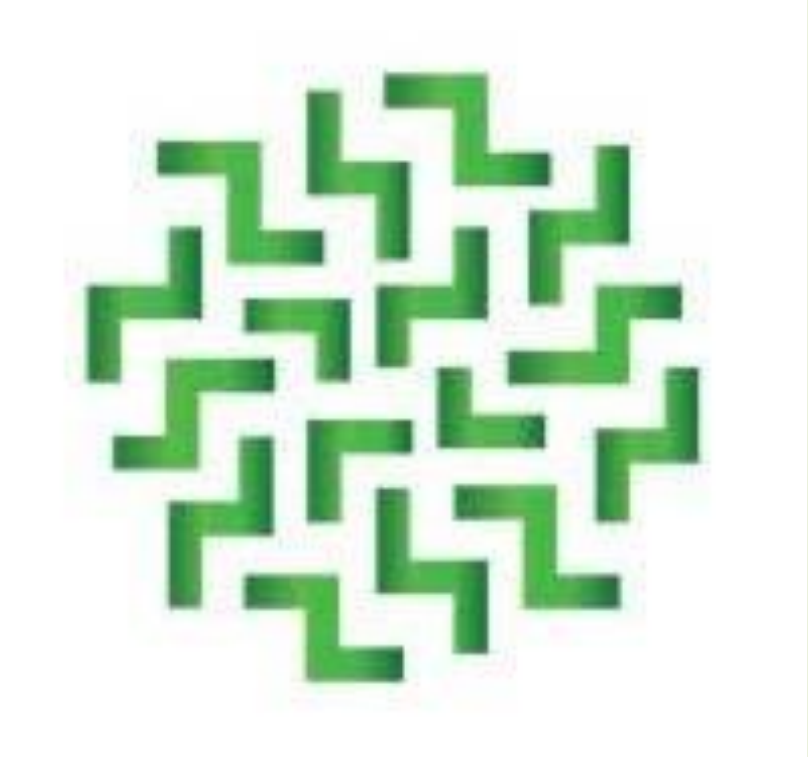
EMRChains Healthcare System

Governance, Risk, and Compliance (GRC) Report



Created By: **Ahmed Umar Rehman**

Date: 11/07/2025

Version: 1.0

Contents

1 Executive Summary

The EMRChains Healthcare System leverages blockchain technology, AES-GCM encryption, and role-based access control to manage electronic medical records (EMR) securely. This report evaluates the system's compliance with Pakistani healthcare standards, global regulations (e.g., HIPAA, GDPR), and industry best practices. The system demonstrates partial compliance with moderate risk exposure due to vulnerabilities in clipboard monitoring, file encryption handling, and incomplete incident response procedures. Key strengths include robust encryption and blockchain-based audit logging, but gaps in granular access controls and regulatory alignment require immediate attention.

Compliance Status: Partial compliance with moderate risk exposure
Major Risk Areas:

- Incomplete clipboard monitoring implementation
- Inconsistent file encryption handling
- Lack of formal incident response procedures
- Absence of comprehensive data protection policies aligned with Pakistani regulations

Key Governance Structures:

- Biometric and two-factor authentication
- AES-GCM encryption for data security
- Blockchain-based immutable audit trails

Recommendations:

- Address vulnerabilities in clipboard monitoring and file encryption
- Develop formal incident response and data protection policies
- Align with emerging Pakistani data protection laws (e.g., Draft PDP Act)

2 Introduction

The EMRChains Healthcare System aims to enhance patient data security through blockchain technology, advanced encryption (AES-GCM), and role-based access controls. This GRC report assesses the system's adherence to Pakistani healthcare regulations, such as the Drug Regulatory Authority of Pakistan (DRAP) Act and the Drugs Act, 1976, as well as global standards like HIPAA and GDPR, which are relevant due to international partnerships and data-sharing practices. The report evaluates governance structures, identifies risks, and ensures compliance

with data security standards, particularly in the absence of a comprehensive data protection law in Pakistan.

3 Governance Assessment

3.1 Security Policies and Procedures

The system incorporates security measures but lacks comprehensive policies aligned with Pakistani standards.

Policy Area	Status	Notes
Data Encryption	Implemented	AES-GCM encryption used, but inconsistent file extension handling (.enc)
Authentication	Implemented	Biometric and two-factor authentication implemented
Audit Logging	Implemented	Blockchain-based audit logging provides immutable records
Data Access	Partial	Role-based access controls lack granularity for specific roles
Incident Response	Missing	No documented incident response procedures
Data Protection Policy	Missing	No policy addressing data collection, storage, and sharing per Draft PDP Act

Table 1: Security Policies and Procedures

Gap Analysis: The absence of a formal data protection policy is critical, given Pakistan's lack of comprehensive data protection legislation. The Draft Personal Data Protection Act (PDP Act) is under consideration, and policies should align with its proposed requirements for data processing and cross-border transfers. Incident response procedures are essential for compliance with global standards like HIPAA, which mandates documented plans for security incidents.

3.2 Roles and Responsibilities

The system defines roles through specialized dashboards (Doctor, Patient) but lacks clear documentation of security responsibilities.

Gap: No explicitly defined Security Officer role with documented responsibilities for overseeing compliance and incident management, which is critical for aligning with best practices.

3.3 Management Oversight

The `AuditLogs.tsx` component provides a foundation for oversight through blockchain-based logging, but gaps include:

Role	Responsibilities	Status
System Administrators	Manage authentication and user access	Defined
Healthcare Providers	Access and share patient data appropriately	Defined
Security Officers	Oversee audit logs and compliance (implied)	Undefined

Table 2: Roles and Responsibilities

- No documented review cycles for security incidents
- Lack of a security metrics dashboard for real-time monitoring
- Undefined escalation procedures for security events

Recommendation: Implement a centralized GRC dashboard to track compliance metrics and security incidents, aligning with industry best practices for continuous monitoring.

4 Risk Assessment

4.1 Security Vulnerabilities

Vulnerability	Severity	Description
Clipboard Monitoring	High	TypeScript errors and incomplete event handling in clipboard monitoring service
File Extension Handling	Medium	Inconsistent use of .enc extension for encrypted files
Password Validation	Low	Basic validation exists but lacks NIST 800-63B compliance
Suspicious Address Detection	Medium	Limited patterns for detecting suspicious blockchain wallet addresses

Table 3: Security Vulnerabilities

4.2 Data Encryption Practices

The system uses AES-GCM authenticated encryption, suitable for healthcare data.

Strengths:

- Implementation of AES-GCM authenticated encryption
- Password-based encryption with validation

- Support for multiple file types (PDF, TXT, JSON)

Weaknesses:

- Inconsistent file extension handling
- Lack of key management system
- No key rotation policy evident in the code

4.3 Access Control Mechanisms

The system implements multi-layer authentication:

1. `BiometricLogin.tsx` – Biometric authentication capability
2. `TwoFactorAuth.tsx` – Additional verification layer
3. `LoginForm.tsx` – Traditional credential-based access

Gaps:

- No session timeout mechanisms visible in the code
- Limited granular permission settings for different user roles
- Absence of context-aware access controls

4.4 Technical Debt Analysis

Component	Technical Debt	Impact
Clipboard Monitoring	High	Missing property declarations cause TypeScript errors
Encryption Service	Medium	Duplicated logic for file extension handling
UI Components	Low	Modal and Badge components lack accessibility features
Wallet Integration	Medium	Limited validation of wallet addresses

Table 4: Technical Debt Analysis

Regulation	Compliance Status	Gap Analysis
DRAP Act	Partial	Lacks specific guidelines for EMR security but requires general compliance
Drugs Act, 1976	Partial	No explicit EMR requirements; general data security applies
Draft PDP Act	Not Implemented	No policy for data processing and cross-border transfers

Table 5: Pakistani Healthcare Regulations

Regulation	Compliance Status	Gap Analysis
HIPAA	Partial	Encryption implemented but audit controls incomplete
GDPR	Partial	Data protection mechanisms exist but consent management unclear
HITECH	Partial	Electronic records security implemented but breach notification absent

Table 6: Global Healthcare Standards

5 Compliance Status

5.1 Pakistani Healthcare Regulations

5.2 Global Healthcare Standards (HIPAA, GDPR)

5.3 Industry Best Practices

Best Practice	Status	Notes
Zero Trust Architecture	Partial	Multi-factor authentication exists but network segmentation unclear
Principle of Least Privilege	Partial	Role-based access exists but granular controls limited
Defense in Depth	Partial	Multiple security layers but gaps in implementation

Table 7: Industry Best Practices

6 Detailed Findings

6.1 Specific Vulnerabilities

1. **Clipboard Monitoring Implementation (High)**
   - TypeScript errors due to missing property declarations
   - Limited event handling for clipboard events
   - **Recommendation:** Complete implementation with proper TypeScript definitions
2. **File Encryption Extension Handling (Medium)**
   - Inconsistent application of .enc extension
   - **Recommendation:** Standardize file handling logic
3. **Password Validation (Low)**
   - Basic validation exists but could be strengthened
   - **Recommendation:** Implement NIST 800-63B compliant password policies
4. **Suspicious Blockchain Address Detection (Medium)**
   - Limited patterns for detecting suspicious addresses
   - **Recommendation:** Expand detection patterns and implement real-time verification

6.2 Security Measures Implemented

1. **AES-GCM Encryption**
   - Provides authenticated encryption
   - **Recommendation:** Add key rotation mechanism
2. **Biometric Authentication**
   - Provides strong user verification
   - **Recommendation:** Ensure compliance with biometric data regulations
3. **Blockchain Integration**
   - Provides immutable audit trail

- **Recommendation:** Implement additional transaction validation

4. **Two-Factor Authentication**
   - Adds security layer to authentication
   - **Recommendation:** Support hardware security keys (FIDO2/WebAuthn)

6.3 Recommendations for Improvement

6.3.1 Immediate Actions (0-30 days)

1. Fix TypeScript errors in clipboard monitoring service
2. Standardize file extension handling for encrypted files
3. Implement comprehensive error handling for encryption/decryption

6.3.2 Short-term Improvements (1-3 months)

1. Develop and document incident response procedures
2. Implement session timeout mechanisms
3. Enhance password policies with NIST recommendations
4. Add data classification schema

6.3.3 Long-term Enhancements (3-6 months)

1. Implement comprehensive key management system
2. Develop security metrics dashboard
3. Implement zero trust architecture principles
4. Add advanced threat detection for blockchain operations

7 Appendix: Technical Implementation Review

7.1 Clipboard Monitoring Service

The clipboard monitoring service (`clipboardMonitoring.ts`) is designed to detect suspicious blockchain wallet addresses but has implementation issues:

```
export class ClipboardMonitoringService {
    private isMonitoring = false;
    private lastClipboardContent = '';
    private alertSound: HTMLAudioElement | null = null;

// Missing property declarations fixed but implementation incomplete
}
```

7.2 Encryption Service

The encryption service (`encryption.ts`) implements AES-GCM but has inconsistent file handling:

```
encryptFile(file: File, password: string): Promise<EncryptedFile> {
    // Implementation needs consistent .enc extension handling
}
```

7.3 Blockchain Integration

The blockchain integration provides immutable audit trails but lacks advanced validation:

- **Strength:** Immutable record keeping
- **Weakness:** Limited address validation
- **Recommendation:** Enhance real-time transaction validation

8 References

- Digital Health Laws and Regulations Report 2024-2025 Pakistan
- Summary of the HIPAA Security Rule
- Securing patient data in the healthcare industry
- Patient Data Privacy: The Role of Cybersecurity in Healthcare
- HIPAA Encryption Requirements - 2025 Update
- Top 12 Healthcare GRC software in 2025