Applying the Risk Management Framework (RMF) to a Critical System

Group members: Nithyasree Atmakuru-801391204, Ana Sharma- 801432222, Alexis Diamond- 801181831

Step 1: Categorize the Information System

Objective:

Determine the security category of XYZ Healthcare's EHR system by assessing the potential impact of a security breach on **confidentiality (C), integrity (I), and availability (A**) using FIPS 199 (NIST, 2004).

Security Categorization

The security category is expressed as SC = {(Confidentiality, Impact), (Integrity, Impact), (Availability, Impact)}, with impact levels of **Low, Moderate, or High**.

1. **Confidentiality (C):**

   Impact: High

   Justification: The EHR system stores Protected Health Information (PHI). Unauthorized disclosure could cause severe harm, including identity theft, financial fraud, and legal penalties. FIPS 199 defines High impact as causing severe or catastrophic harm (NIST, 2004).

2. **Integrity (I):**

Impact: High

Justification: Tampering with patient data could lead to incorrect diagnoses, treatment errors, or legal liabilities. FIPS 199 defines High impact as causing severe or catastrophic harm (NIST, 2004).

3. **Availability (A):**

   Impact: Moderate

   Justification: Downtime could disrupt healthcare operations, but redundancy and failover mechanisms mitigate prolonged outages. FIPS 199 defines Moderate impact as causing degraded operations or financial losses (NIST, 2004).

Final Security Category

SC = {(Confidentiality, High), (Integrity, High), (Availability, Moderate)}

Abbreviated as **High-High-Moderate (HHM**).

Step 2: Select Security Controls

Based on the High-High-Moderate (HHM) categorization, the following security controls are selected from NIST SP 800-53 (NIST, 2020):

1. Access Control (AC):

1. AC-2: Account Management

Why Necessary: Ensures proper creation, modification, and disabling of user accounts.

Risk Addressed: Prevents unauthorized access to PHI by managing user accounts effectively.

2. AC-3: Access Enforcement:

Why Necessary: Restricts access to authorized users based on roles.

Risk Addressed: Ensures only authorized personnel can access sensitive patient data.

3. AC-6: Least Privilege:

Why Necessary: Limits user permissions to the minimum necessary.

Risk Addressed: Reduces the risk of insider threats and accidental data exposure.

4. AC-7: Unsuccessful Login Attempts

Why Necessary: Locks accounts after multiple failed login attempts.

Risk Addressed: Prevents brute-force attacks on the EHR system.

5. AC-17: Remote Access:

Why Necessary: Secures remote access using encryption and multi-factor authentication (MFA).

Risk Addressed: Protects against unauthorized remote access to PHI.

2. Audit and Accountability (AU):

1. AU-2: Auditable Events

Why Necessary: Logs all access and modification events.

Risk Addressed: Provides a trail for detecting and investigating unauthorized activities.

2. AU-3: Content of Audit Records

Why Necessary: Ensures logs include sufficient detail for forensic analysis.

Risk Addressed: Supports incident response and compliance audits.

3. AU-6: Audit Review, Analysis, and Reporting

Why Necessary: Regularly reviews logs for suspicious activity.

Risk Addressed: Detects and mitigates potential security incidents.

4. AU-12: Audit Generation

Why Necessary: Automates log generation for all system events.

Risk Addressed: Ensures comprehensive monitoring of the EHR system.

5. AU-14: Session Audit

Why Necessary: Tracks user sessions in real-time.

Risk Addressed: Identifies unauthorized or suspicious user activity.

3. System and Communications Protection (SC):

1. SC-7: Boundary Protection

Why Necessary: Implements firewalls and intrusion detection/prevention systems (IDS/IPS).

Risk Addressed: Protects the EHR system from external attacks.

2. SC-8: Transmission Confidentiality and Integrity

Why Necessary: Encrypts data in transit using TLS.

Risk Addressed: Prevents interception or tampering with patient data during transmission.

3. SC-12: Cryptographic Key Management

Why Necessary: Secures cryptographic keys used for encryption.

Risk Addressed: Ensures the integrity and confidentiality of encrypted data.

4. SC-28: Protection of Information at Rest

Why Necessary: Encrypts stored patient data.

Risk Addressed: Protects PHI from theft or unauthorized access.

5. SC-39: Process Isolation

Why Necessary: Ensures the EHR system operates in a secure, isolated environment.

Risk Addressed: Prevents unauthorized processes from accessing sensitive data.

4. Contingency Planning (CP):

1. CP-2: Contingency Plan

Why Necessary: Develop a plan for responding to system disruptions.

Risk Addressed: Ensures continuity of operations during emergencies.

2. CP-6: Alternate Storage Site

Why Necessary: Maintains a backup site for data recovery.

Risk Addressed: Protects against data loss due to system failures or disasters.

3. CP-9: Information System Backup

Why Necessary: Regularly backs up EHR data.

Risk Addressed: Ensures data recovery in case of corruption or loss.

4. CP-10: Information System Recovery and Reconstitution

Why Necessary: Ensures rapid recovery after an incident.

Risk Addressed: Minimizes downtime and disruption to healthcare operations.5.

5.CP-11: Alternate Communications Protocols

Why Necessary: Provides alternative communication methods during outages.

Risk Addressed Ensures continued access to the EHR system during disruptions.

3. Develop a Risk Assessment Report (Steps 3 & 4):

Risk Matrix:

RISK	**LIKELIHOOD**	**IMPACT**	**RISK LEVEL**
DATA BREACH	**HIGH**	**HIGH**	**HIGH**
INSIDER THREAT	**MEDIUM**	**HIGH**	**MEDIUM**
DENIAL OF SERVICE (DOS)	**MEDIUM**	**MEDIUM**	**MEDIUM**

Mitigation Strategies:

1. Data Breach:

   Risk: Unauthorized access to PHI.

Mitigation: Implement AC-2 (Account Management) and SC-28 (Protection of Information at Rest) to restrict access and encrypt data.

2. Insider Threat:

   Risk: Malicious or accidental misuse of access by employees.

   Mitigation: Enforce AU-6 (Audit Review) and AC-6 (Least Privilege) to monitor and limit user actions.

3. Denial of Service (DoS):

   Risk: Disruption of EHR system availability.

   Mitigation: Use SC-7 (Boundary Protection) and CP-10 (Information System Recovery) to detect and recover from attacks.

Step.5. Authorization Package

The EHR system meets most security requirements, but gaps exist in cryptographic key management (SC-12) and audit log retention (AU-11).

Security Assessment Report (SAR):

The EHR system meets most security requirements, but gaps exist in cryptographic key management (SC-12) and audit log retention (AU-11).

Findings:

1. SC-12: Cryptographic keys are not rotated frequently.

2. AU-11: Audit logs are retained for only 30 days instead of the required 90 days.

3. AC-17: MFA is not enforced for all remote access.

Plan of Action and Milestones (POA&M):

1. Gap: SC-12 – Key rotation not compliant.

Action: Implement automated key rotation every 90 days.

Milestone: Complete within 60 days.

2. Gap: AU-11 – Insufficient log retention.

Action: Extend log retention to 90 days.

Milestone: Complete within 30 days.

3. Gap: AC-17 – MFA not enforced.

Action: Enable MFA for all remote access.

Milestone: Complete within 45 days.

Step 6. Continuous Monitoring Plan

Frequency of Control Assessments: Quarterly reviews of all controls.

Automated Tools: Use SIEM (Security Information and Event Management) tools for real-time monitoring.

Reporting Mechanisms: Establish an incident response team and reporting structure for security incidents.

Control Baselines: Refer to **NIST SP 800-53B** for baseline updates and adjustments (NIST, 2020).

References

- National Institute of Standards and Technology (NIST). (2004). **FIPS 199: Standards for Security Categorization of Federal Information and Information Systems.**

- National Institute of Standards and Technology (NIST). (2020). **NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations.**

- National Institute of Standards and Technology (NIST). (2020). **NIST SP 800-53A: Assessing Security and Privacy Controls in Information Systems and Organizations**.

- National Institute of Standards and Technology (NIST). (2020). **NIST SP 800-53B: Control Baselines for Information Systems and Organizations.**