Security Assessment & Risk Mitigation Plan

Brylan Williamson
Security+ Certification 2026SP-CYBR-1200-B500
Instructor: Gina Llanos Cramer
Final Date: 2/26/2026

1. Executive Summary

This report presents a security assessment and risk mitigation plan for a fictional mid-sized healthcare organization, “ClearView Health Services,” operating in a primarily cloud-based environment. The organization employs approximately 200 staff members, including healthcare providers, administrative personnel, and remote billing specialists.

Due to the sensitive nature of protected health information (PHI), healthcare organizations are frequent targets of phishing campaigns, ransomware attacks, insider threats, and credential compromise. ClearView Health Services currently relies heavily on cloud-hosted electronic health record (EHR) systems, email platforms, and remote access solutions.

This assessment identifies key assets, threats, and vulnerabilities and recommends layered administrative, technical, and physical security controls. The proposed controls align with Security+ principles and industry-recognized cybersecurity frameworks to reduce risk, improve resilience, and ensure operational continuity.

2. Organizational Overview

Organization Name: ClearView Health Services (Fictional)
Industry: Healthcare
Employees: ~200
Environment: Primarily cloud-based with limited on-premise networking equipment

Infrastructure Overview

- Cloud hosted EHR system
- Cloud email platform
- Remote workforce using VPN
- On site wireless network for clinical staff
- Encrypted laptops for providers
- Limited on-prem network switches and firewall appliance

Sensitive Data Handled

- Protected Health Information
- Personally Identifiable Information
- Insurance and billing records
- Internal HR data

Because healthcare data is highly valuable on the black market, the organization faces elevated cybersecurity risk.

3. Risk Assessment

Critical Assets

- Electronic Health Record database
- Cloud identity management system
- Email system
- Endpoint devices
- Backup systems

Identified Threats

- Phishing and social engineering attacks

- Ransomware
- Insider threats
- Credential stuffing attacks
- Cloud misconfiguration exploitation

Identified Vulnerabilities

- Weak password complexity enforcement
- Lack of MFA
- Inconsistent patch management
- Limited user security awareness training
- Over permissioned user accounts

Risk Analysis Example

Risk: Phishing leading to credential compromise
Likelihood: High
Impact: High
Risk Level: High

Without MFA enforcement, compromised credentials could allow unauthorized access to PHI stored in cloud systems, resulting in regulatory penalties, reputational damage, and operational disruption.

4. Security Controls Implementation

Administrative Controls

1. Security Awareness Training

Mandatory quarterly phishing awareness and data protection training will reduce social engineering success rates.

2. Acceptable Use Policy

Defines appropriate system usage and establishes accountability.

3. Access Control Policy

Implements least privilege and RBAC.

4. Incident Response Plan

Formal documentation of response procedures ensures rapid containment and recovery.

Technical Controls

1. Multi-Factor Authentication (MFA)

MFA will be required for all cloud logins and VPN access.
This mitigates credential based attacks such as phishing and password spraying.

2. Endpoint Detection & Response (EDR)

Deploy EDR to monitor endpoints for suspicious behavior and ransomware indicators.

3. Next Generation Firewall (NGFW)

Provides deep packet inspection and intrusion prevention capabilities.

4. Encryption

- AES-256 encryption for data at rest
- TLS 1.2+ for data in transit

5. Patch Management Automation

Automated cloud-based patching reduces exposure to known vulnerabilities.

6. Cloud Configuration Monitoring

Continuous monitoring to detect misconfigured storage buckets or excessive permissions.

Physical Controls

- Badge-based facility access
- Locked server/network closets
- CCTV monitoring
- Visitor sign in procedures

Although infrastructure is mostly cloud based, physical controls remain important for endpoint and network hardware protection.

5. Incident Response Plan

The organization will follow a structured six phase model:

1. Preparation

- Staff training
- Logging and monitoring enabled
- Backup validation

2. Identification

- SIEM alerts
- User reported suspicious emails
- EDR threat detection

3. Containment

- Isolate infected endpoints
- Disable compromised accounts
- Block malicious IP addresses

4. Eradication

- Remove malware
- Patch exploited vulnerabilities
- Reset credentials

5. Recovery

- Restore systems from clean backups
- Monitor for reinfection
- Validate system integrity

6. Lessons Learned

- Conduct post incident review
- Update policies
- Improve detection rules

This structured approach reduces downtime and limits damage.

6. Business Continuity & Disaster Recovery

Healthcare operations must remain available to protect patient safety.

Backup Strategy (3-2-1 Rule)

- 3 copies of critical data
- 2 different storage types
- 1 offsite immutable cloud backup

Recovery Time Objective (RTO)

Target: 4 hours for critical EHR systems.

Recovery Point Objective (RPO)

Target: 1 hour maximum data loss.

Redundancy Measures

- Cloud region redundancy
- High availability configurations
- Failover network connectivity

These measures reduce operational impact during cyber incidents or outages.

7. Governance & Compliance Alignment

The recommended controls align with:

- NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover)
- ISO/IEC 27001 security control principles
- CompTIA Security+ domain objectives

The risk management process follows structured identification and mitigation principles consistent with recognized industry best practices.

8. Conclusion

ClearView Health Services faces elevated cybersecurity risk due to its reliance on cloud infrastructure and the sensitive nature of healthcare data. Through implementation of layered administrative, technical, and physical controls, the organization can significantly reduce the likelihood and impact of cyber threats.

By enforcing least privilege, deploying MFA, strengthening endpoint monitoring, and establishing a formal incident response process, the organization improves its security posture while maintaining operational efficiency.

This assessment demonstrates applied Security+ knowledge through practical risk evaluation, control selection, and alignment with industry frameworks.