Risk Assessment Report – HealthyLife Clinic

(Fictional Healthcare Clinic, using NIST Cybersecurity Framework)

1. Introduction

HealthyLife Clinic depends on technology to deliver patient care, store medical records, and handle billing. This risk assessment was conducted to evaluate threats to the clinic's critical systems and data. The assessment follows the NIST Cybersecurity Framework (CSF) to identify risks, score their impact and likelihood, and recommend improvements.

The goal is to strengthen the clinic's overall security posture, reduce exposure to cyber threats, and ensure compliance with healthcare regulations.

2. Methodology

Framework Used: NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover).

Process:
1. Identified key assets (patient records, staff laptops, billing systems, Wi-Fi, cloud storage).
2. Listed realistic threats and vulnerabilities.
3. Assigned Impact (High, Medium, Low) and Likelihood (High, Medium, Low).
4. Calculated Risk Score = Impact × Likelihood.
5. Mapped risks to NIST CSF functions and created mitigation steps.

Deliverables: Risk Register (Excel file) and this summary report.

3. Key Findings

R1 – Ransomware on Patient Records

Impact: High | Likelihood: Medium | Risk Score: 6

Issue: Unpatched systems could be encrypted by ransomware.

Recommendation: Maintain daily backups, patch regularly, use anti-malware.

R2 – Phishing Attacks on Staff

Impact: High | Likelihood: High | Risk Score: 9 (Critical)

Issue: Staff may click phishing emails and give away login credentials.

Recommendation: Enable MFA, provide phishing awareness training, block suspicious domains.

R3 – Lost or Stolen Doctor Laptop

Impact: High | Likelihood: Medium | Risk Score: 6

Issue: Laptops with patient health information (PHI) may be lost or stolen.

Recommendation: Enforce full disk encryption, remote wipe, auto-lock screens.

R4 – Guest Wi-Fi Not Segmented

Impact: Medium | Likelihood: Medium | Risk Score: 4

Issue: Guest Wi-Fi could allow attackers to move into the internal network.

Recommendation: Separate guest/internal Wi-Fi, enforce WPA3, rotate passwords.

R5 – Vendor Data Breach (Billing System)

Impact: High | Likelihood: Medium | Risk Score: 6

Issue: Third-party billing vendor could be compromised.

Recommendation: Conduct vendor risk assessments, review contracts, limit shared data.

4. Recommendations

1. Technical Controls
- Patch management, antivirus, encryption, multi-factor authentication.
- Network segmentation and improved backup strategy.

2. Administrative Controls
- Phishing and security awareness training for all staff.
- Stronger offboarding process for employees.

3. Incident Response & Recovery
- Develop an incident response plan.
- Run tabletop exercises to test readiness.
- Document clear escalation paths.

5. Conclusion

This assessment shows that HealthyLife Clinic faces real but manageable risks. By addressing phishing, ransomware, device security, and vendor management, the clinic can significantly reduce its exposure. Using the NIST CSF, the clinic now has a roadmap to strengthen its security posture, improve compliance, and protect patient trust.

Next steps include reviewing risks quarterly, updating the register, and re-testing controls as the clinic's environment changes.