Security Strategy Proposal for HealthFirst Medical

1. Executive Summary

HealthFirst Medical is a mid-sized healthcare organization experiencing rapid digital growth. With the increase in digital records, telehealth services, and patient data access, the company faces heightened cybersecurity risks especially ransomware, phishing, and regulatory compliance violations. This proposal outlines a comprehensive cybersecurity strategy addressing vulnerabilities across people, processes, and technology to safeguard HealthFirst Medical's operations and patient trust.

2. Company Background

HealthFirst Medical operates five clinics and one central administration office. The organization manages over 50,000 patient records, utilizes a cloud-based EHR (Electronic Health Records) system, and recently adopted a third-party telehealth platform. The IT team includes five personnel, and there is no current full-time security specialist.

3. Security Challenges Identified

- Unsecured legacy systems in use at several clinics.
- Lack of multi-factor authentication for remote access.
- Minimal employee cybersecurity awareness training.
- No formal incident response plan or SIEM solution.
- Inconsistent firewall and patch management practices.

4. Recommended Improvements

A. People

- Conduct quarterly cybersecurity awareness training.
  Topics: phishing, malware prevention, password hygiene, HIPAA data handling.
- Assign a security person within the IT team to oversee risk assessments and track compliance.

B. Processes

- Develop a formal Incident Response Plan with roles, playbooks, and escalation procedures.
- Enforce password policies (min. 12 characters, complexity, regular rotation).
- Implement data access control policies using least-privilege principles.
- Regular audits of system logs and employee access behavior.

C. Technology

- Deploy MFA across VPN, EHR systems, and cloud platforms.
- Implement a SIEM solution such as Splunk or Microsoft Sentinel for log analysis and threat detection.
- Upgrade firewalls and enable intrusion detection.
- Automated patch management tools for operating systems and applications.
- Secure and encrypt mobile and telehealth data transmission.

5. Implementation Plan

Phase 1	Roll out MFA, firewall upgrades, and password policies	Month 1–2	IT Security Lead
Phase 2	Staff training & security awareness program launch	Month 2–3	HR + IT
Phase 3	Deploy SIEM & develop Incident Response Plan	Month 3–5	External MSSP + IT
Phase 4	Quarterly audits, metrics reviews, & policy enforcement	Ongoing	Security professional

6. Conclusion

HealthFirst Medical must prioritize cybersecurity to protect its patients, data, and reputation. The strategy laid out in this proposal provides a roadmap to build a mature security program through technical controls, employee empowerment, and ongoing process improvements.

Prepared by: Rodney Hall
Date: May,10, 2025