Cybersecurity Policy for Healthcare (Low Risk Environment)

--1. Introduction--

This Cybersecurity Policy outlines the framework for protecting the confidentiality, integrity, and availability of Protected Health Information (PHI) and other sensitive data within [Organization Name]. This policy applies to all employees, contractors, vendors, and any other individuals or entities accessing or using [Organization Name]'s information systems, regardless of location or device. Given the organization's classification as a "low risk" environment, the controls outlined in this policy are designed to provide reasonable and appropriate security measures, aligned with industry best practices and regulatory requirements, while maintaining operational efficiency. This policy is developed in accordance with the Risk Management Framework (RMF) and is intended to support [Organization Name]'s mission to provide quality healthcare services while safeguarding patient information.

--2. Risk Assessment--

[Organization Name] will conduct periodic risk assessments, at least annually, to identify, analyze, and evaluate potential threats and vulnerabilities to our information systems and data. These assessments will consider both internal and external risks, including but not limited to:

- --Data breaches:-- Unauthorized access, use, or disclosure of PHI.
- --Malware infections:-- Viruses, ransomware, and other malicious software impacting system availability and data integrity.
- --Insider threats:-- Intentional or unintentional actions by employees or contractors that compromise security.
- --Physical security breaches:-- Unauthorized access to facilities housing information systems.
- --Software vulnerabilities:-- Exploitable flaws in software applications and operating systems.

The risk assessment process will include identifying assets, threats, vulnerabilities, likelihood of occurrence, and potential impact. The results of the risk assessment will be used to prioritize security controls and inform ongoing security efforts. Remediation plans will be documented and tracked.

--3. Data Protection--

Protecting sensitive data is paramount. The following measures will be implemented to safeguard PHI and other confidential information:

- --Data Encryption:-- PHI in transit and at rest will be encrypted using industry-standard encryption algorithms. This includes encrypting data stored on servers, workstations, laptops, and mobile devices.
- --Data Loss Prevention (DLP):-- DLP tools and procedures will be implemented to prevent sensitive data from leaving the organization's control without authorization.
- --Data Backup and Recovery:-- Regular backups of critical data will be performed and stored securely, both on-site and off-site. Recovery procedures will be documented and

tested periodically to ensure data can be restored in a timely manner in the event of a disaster or data loss.
- --Data Minimization:-- Only necessary data will be collected and retained. Data retention policies will be established and followed to ensure that data is securely disposed of when it is no longer needed.
- --Data Classification:-- Data will be classified based on its sensitivity and criticality. Appropriate security controls will be applied based on the data classification level.

--4. Access Controls--

Access to information systems and data will be restricted based on the principle of least privilege. Only authorized personnel will be granted access to the information they need to perform their job duties.

- --User Authentication:-- Strong authentication methods, such as multi-factor authentication (MFA), will be implemented for all users accessing sensitive systems and data.
- --Role-Based Access Control (RBAC):-- Access rights will be assigned based on job roles and responsibilities.
- --Account Management:-- User accounts will be created, modified, and terminated promptly and securely. Regular reviews of user access rights will be conducted to ensure accuracy and appropriateness.
- --Password Management:-- Strong password policies will be enforced, including requirements for password complexity, length, and regular changes. Password reuse will be prohibited.
- --Remote Access:-- Secure remote access methods, such as VPNs, will be used for accessing the organization's network and systems from remote locations.

--5. Incident Response--

[Organization Name] will maintain a comprehensive Incident Response Plan (IRP) to effectively detect, respond to, and recover from security incidents. The IRP will include:

- --Incident Identification and Reporting:-- Procedures for identifying and reporting suspected security incidents.
- --Incident Containment:-- Steps to contain the spread of an incident and prevent further damage.
- --Incident Eradication:-- Actions to remove the cause of the incident and restore systems to a secure state.
- --Incident Recovery:-- Procedures for restoring data, systems, and services to normal operation.
- --Post-Incident Analysis:-- A review of the incident to identify lessons learned and improve security controls.

The IRP will be tested periodically through tabletop exercises and simulations. All employees will be trained on their roles and responsibilities in the event of a security incident.

--6. Security Awareness Training--

All employees, contractors, and vendors will receive regular security awareness training

to educate them on security risks and best practices. Training topics will include:

- --Phishing awareness:-- Identifying and avoiding phishing attacks.
- --Malware prevention:-- Recognizing and preventing malware infections.
- --Password security:-- Creating and maintaining strong passwords.
- --Data protection:-- Handling sensitive data securely.
- --Incident reporting:-- Reporting suspected security incidents.
- --Physical security:-- Maintaining a secure physical environment.
- --Social Engineering:-- Recognizing and avoiding social engineering tactics

Training will be tailored to the specific roles and responsibilities of employees. Completion of security awareness training will be mandatory.

--7. Compliance and Auditing--

[Organization Name] is committed to complying with all applicable laws, regulations, and industry standards, including those related to the Risk Management Framework (RMF).

- --Regular Audits:-- Periodic internal and external audits will be conducted to assess compliance with this policy and other security requirements.
- --Vulnerability Scanning:-- Regular vulnerability scans will be performed on information systems to identify and remediate security vulnerabilities.
- --Penetration Testing:-- Periodic penetration testing will be conducted to simulate real-world attacks and identify weaknesses in security controls.
- --Policy Review:-- This policy will be reviewed and updated at least annually or more frequently as needed to address changes in the threat landscape, regulatory requirements, or business operations.
- --RMF Alignment:-- Security controls implemented under this policy will map directly to the control families and individual controls defined within the Risk Management Framework (RMF). Control implementation status will be continuously monitored and reported.

--8. Conclusion--

This Cybersecurity Policy is a critical component of [Organization Name]'s commitment to protecting sensitive data and ensuring the security of our information systems. By adhering to this policy, all employees, contractors, and vendors contribute to maintaining a secure and compliant environment. This policy is subject to change and will be reviewed periodically to ensure it remains effective and aligned with industry best practices and regulatory requirements. All personnel are responsible for understanding and complying with this policy.