Cybersecurity Policy for Healthcare Organizations (Low Risk Environment)

--1. Introduction--

This Cybersecurity Policy outlines the minimum-security requirements for protecting the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI) and other sensitive data within this healthcare organization. This policy is designed to establish a baseline of security controls commensurate with a low-risk environment, while adhering to applicable regulatory requirements, including the Risk Management Framework (RMF). All employees, contractors, vendors, and any other individuals or entities accessing or using the organization's information systems are required to comply with this policy. This policy will be reviewed and updated at least annually, or more frequently as required by changes in technology, regulations, or business needs.

--2. Risk Assessment--

Recognizing that even in a low-risk environment, vulnerabilities exist, this organization will conduct a periodic risk assessment to identify potential threats, vulnerabilities, and the resulting impact on ePHI and other sensitive data.

- --Frequency:-- A risk assessment will be conducted at least annually, and after any significant changes to the organization's IT infrastructure, applications, or business processes.
- --Scope:-- The risk assessment will encompass all information systems, devices, and networks that store, process, or transmit ePHI or other sensitive data.
- --Methodology:-- The risk assessment will utilize a recognized framework, such as NIST Special Publication 800-30 (Guide for Conducting Risk Assessments).
- --Documentation:-- The risk assessment findings, including identified risks, vulnerabilities, and proposed mitigation strategies, will be documented and maintained for audit purposes.
- --Mitigation:-- Risk mitigation strategies will be prioritized based on the likelihood and impact of the identified risks. Lower-priority risks, typical in a "low risk" environment, will be addressed through basic security controls detailed throughout this policy.
- --Review and Approval:-- The risk assessment and mitigation plan will be reviewed and approved by senior management and the CISO (or designated security officer).

--3. Data Protection--

Protecting the confidentiality and integrity of data is paramount. This section outlines data protection requirements for ePHI and other sensitive information.

- --Data Classification:-- All data will be classified based on its sensitivity and criticality. This classification will determine the appropriate level of security controls to be applied. ePHI will be classified as highly sensitive.
- --Data Encryption:-- ePHI stored at rest on laptops or other portable devices must be encrypted using an industry-standard encryption algorithm (e.g., AES). Encryption of ePHI in transit should be prioritized, especially when transmitted outside the organization's network.
- --Data Backup and Recovery:-- Regular backups of ePHI and other critical data will be

performed. Backup data will be stored securely, both onsite and offsite, and tested regularly to ensure recoverability. Backup frequency will be determined based on data criticality and recovery time objectives (RTOs).

- --Data Retention and Disposal:-- Data retention policies will be established and followed to comply with legal and regulatory requirements. Data will be securely disposed of when it is no longer needed, using methods that prevent unauthorized access or recovery (e.g., data wiping, physical destruction).
- --Data Loss Prevention (DLP):-- Implement basic DLP measures, such as monitoring email communications for sensitive information and educating employees on appropriate data handling practices.

--4. Access Controls--

Access to ePHI and other sensitive data will be restricted to authorized individuals based on the principle of least privilege.

- --User Authentication:-- Strong passwords must be used for all user accounts. Passwords must meet minimum complexity requirements (e.g., length, character types) and be changed regularly. Multi-factor authentication (MFA) should be enabled wherever technically feasible and practical.
- --Access Provisioning and Deprovisioning:-- A formal process will be in place for granting and revoking user access to systems and data. Access will be granted based on job roles and responsibilities. Access will be promptly revoked upon termination of employment or change in job role.
- --Role-Based Access Control (RBAC):-- Access to ePHI and other sensitive data will be managed using RBAC, ensuring that users only have access to the information they need to perform their job duties.
- --Remote Access:-- Remote access to the organization's network and systems will be secured using a Virtual Private Network (VPN) or other secure technology. Remote access will be limited to authorized users and devices.
- --Physical Access Controls:-- Physical access to data centers and other sensitive areas will be restricted to authorized personnel. Access will be controlled through methods such as key cards, security badges, or biometric authentication.

--5. Incident Response--

A comprehensive incident response plan will be developed and maintained to address security incidents, including data breaches and other security events.

- --Incident Detection:-- Security monitoring tools and processes will be implemented to detect security incidents in a timely manner.
- --Incident Reporting:-- Employees are required to report any suspected security incidents immediately to the designated security contact or incident response team.
- --Incident Response Plan:-- The incident response plan will outline the steps to be taken in the event of a security incident, including containment, eradication, recovery, and post-incident analysis. The plan will be tested regularly through tabletop exercises or simulations.
- --Data Breach Notification:-- Procedures will be in place to comply with all applicable

data breach notification laws and regulations.

--6. Security Awareness Training--

Security awareness training will be provided to all employees, contractors, and vendors to educate them on security risks and best practices.

- --Training Frequency:-- Security awareness training will be provided annually, and upon hire, to all individuals with access to the organization's information systems.
- --Training Content:-- The training will cover topics such as password security, phishing awareness, malware prevention, data protection, and incident reporting procedures.
- --Training Delivery:-- Training will be delivered through a variety of methods, such as online modules, instructor-led sessions, and security awareness campaigns.
- --Phishing Simulations:-- Periodic phishing simulations will be conducted to test employee awareness and identify areas for improvement.
- --Documentation:-- Records of security awareness training will be maintained for audit purposes.

--7. Compliance and Auditing--

This organization is committed to complying with all applicable laws, regulations, and industry standards, including the Risk Management Framework (RMF).

- --RMF Implementation:-- This organization will implement security controls based on the RMF to ensure the confidentiality, integrity, and availability of ePHI. The security controls will be selected based on a risk-based approach, considering the organization's specific threat environment and business needs.
- --Security Audits:-- Regular security audits will be conducted to assess the effectiveness of security controls and identify areas for improvement.
- --Vulnerability Scanning:-- Regular vulnerability scans will be performed on all information systems to identify and remediate security vulnerabilities.
- --Penetration Testing:-- Penetration testing may be conducted periodically to assess the organization's security posture.
- --Documentation:-- All security policies, procedures, and audit results will be documented and maintained for compliance purposes.

--8. Conclusion--

This Cybersecurity Policy provides a framework for protecting ePHI and other sensitive data within this healthcare organization, aligned with a low-risk environment and RMF compliance. By adhering to the principles outlined in this policy, the organization can reduce its risk of security incidents and maintain the trust of its patients, employees, and partners. This policy is a living document and will be reviewed and updated regularly to ensure its continued effectiveness.