Cybersecurity Policy for Healthcare Organizations (Low Risk Environment)

1. Introduction

This Cybersecurity Policy outlines the essential security controls and practices necessary to protect the confidentiality, integrity, and availability of Protected Health Information (PHI) and other sensitive data within this healthcare organization. This policy applies to all employees, contractors, vendors, and any other individuals or entities accessing or using our information systems. While the organization operates in a low-risk environment, proactive security measures are critical to maintain patient trust, ensure business continuity, and comply with applicable regulations. This policy is aligned with the Risk Management Framework (RMF) to manage and mitigate cybersecurity risks. All personnel are required to adhere to this policy.

2. Risk Assessment

--Purpose:-- To systematically identify, assess, and prioritize cybersecurity risks impacting the organization.

--Policy:--

- A risk assessment will be conducted annually, or more frequently if significant changes occur within the organization's IT infrastructure or regulatory landscape.
- The risk assessment will identify potential threats and vulnerabilities, evaluate the likelihood and impact of potential incidents, and prioritize risks based on their severity.
- The risk assessment methodology will align with the Risk Management Framework (RMF) and will document the process for identifying threats, vulnerabilities, and associated risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation of an information system.
- Identified risks will be documented in a Risk Register, which will include mitigation strategies, responsible parties, and target completion dates.
- The Risk Register will be reviewed and updated regularly to reflect the current threat landscape and the status of mitigation efforts.

3. Data Protection

--Purpose:-- To ensure the confidentiality, integrity, and availability of PHI and other sensitive data.

--Policy:--

- --Data Encryption:-- All PHI stored on portable devices (laptops, USB drives) and transmitted electronically (email, file transfer) must be encrypted using industry-standard encryption algorithms. Stored data at rest on servers should use encryption where feasible and risk-appropriate.
- --Data Backup and Recovery:-- Regular data backups will be performed to ensure data can be restored in the event of a system failure or disaster. Backup data will be stored securely, both on-site and off-site, and tested periodically to verify recoverability.
- --Data Minimization:-- Collect and retain only the minimum amount of PHI necessary for

business operations and legal compliance. Review data retention policies regularly and dispose of data securely when it is no longer needed.

- --Data Loss Prevention (DLP):-- Implement basic DLP measures, such as monitoring network traffic for sensitive data being transmitted outside the organization and educating employees on safe data handling practices.
- --Physical Security:-- Physical access to data centers and other areas where sensitive data is stored must be restricted to authorized personnel only. Implement physical security controls such as locks, alarms, and video surveillance.

4. Access Controls

--Purpose:-- To restrict access to information systems and data to authorized users only.

--Policy:--

- --User Accounts:-- All users must have unique user accounts with strong passwords. Generic or shared accounts are prohibited.
- --Password Management:-- Passwords must meet minimum complexity requirements (e.g., length, character types) and be changed regularly. Multi-factor authentication (MFA) should be implemented where feasible, especially for remote access and privileged accounts.
- --Role-Based Access Control (RBAC):-- Access to information systems and data must be granted based on a user's job role and responsibilities. The principle of least privilege will be followed, granting users only the access necessary to perform their duties.
- --Access Review:-- User access rights will be reviewed periodically (at least annually) to ensure they are still appropriate and necessary.
- --Remote Access:-- Remote access to the organization's network and systems must be secured using VPNs or other secure methods. MFA is required for all remote access.
- --Termination of Access:-- When an employee leaves the organization or changes roles, their access rights must be promptly revoked or modified.

5. Incident Response

--Purpose:-- To establish a plan for responding to and recovering from cybersecurity incidents.

--Policy:--

- An Incident Response Plan (IRP) will be developed and maintained, outlining the procedures for detecting, analyzing, containing, eradicating, and recovering from cybersecurity incidents.
- The IRP will include clearly defined roles and responsibilities for incident response team members.
- All employees are responsible for reporting suspected security incidents to the designated incident response team.
- The IRP will be tested periodically through table-top exercises or simulations to ensure its effectiveness.
- Following a security incident, a post-incident review will be conducted to identify lessons learned and improve the IRP.
- Incident Reporting should include event logging, vulnerability scanning and remediation,

and communication with internal and external stakeholders.

6. Security Awareness Training

--Purpose:-- To educate employees on cybersecurity threats and best practices.

--Policy:--

- All employees will receive initial security awareness training upon hire and annual refresher training.
- Training will cover topics such as phishing awareness, password security, data protection, and incident reporting.
- Training will be tailored to the specific risks and vulnerabilities relevant to the organization's operations.
- The effectiveness of security awareness training will be evaluated through quizzes or other assessments.
- Phishing simulations will be conducted periodically to test employee awareness and identify areas for improvement.

7. Compliance and Auditing

--Purpose:-- To ensure compliance with applicable regulations and policies.

--Policy:--

- The organization will comply with all applicable laws and regulations, including the Risk Management Framework (RMF).
- Regular internal audits will be conducted to assess compliance with this Cybersecurity Policy and identify areas for improvement.
- External audits will be conducted as required by regulatory bodies or contractual obligations.
- Audit findings will be documented and addressed in a timely manner.
- The CISO is responsible for maintaining documentation related to compliance efforts and audit results.

8. Conclusion

This Cybersecurity Policy is a living document that will be reviewed and updated regularly to reflect changes in the threat landscape, technology, and regulatory requirements. By adhering to this policy, we can protect our organization's information assets, maintain patient trust, and ensure business continuity. All employees are responsible for upholding the principles and practices outlined in this policy.