Cybersecurity Policy for Healthcare Organization (Low Risk Environment)

1. Introduction

This Cybersecurity Policy outlines the mandatory security standards and practices for [Organization Name] (hereafter referred to as "the Organization") to protect the confidentiality, integrity, and availability of Protected Health Information (PHI) and other sensitive data. This policy applies to all employees, contractors, vendors, and other individuals or entities accessing or using the Organization's information systems and data, irrespective of location. The Organization acknowledges that while classified as a "low-risk environment" based on current infrastructure and data sensitivity assessments, adherence to these policies is critical to maintaining this risk profile and preventing potential security incidents. This policy is designed to be compliant with the National Institute of Standards and Technology (NIST) cybersecurity framework.

2. Risk Assessment

The Organization will conduct a comprehensive risk assessment at least annually, or more frequently if significant changes occur to the IT environment, business operations, or regulatory landscape. This assessment will:

- Identify assets: Identify all critical assets, including hardware, software, data, and physical locations.
- Identify threats and vulnerabilities: Identify potential threats (e.g., malware, phishing, insider threats) and vulnerabilities (e.g., unpatched software, weak passwords) that could compromise the confidentiality, integrity, or availability of these assets.
- Analyze likelihood and impact: Evaluate the likelihood of a threat exploiting a vulnerability and the potential impact on the Organization if such an event were to occur.
- Prioritize risks: Prioritize risks based on their potential impact and likelihood, focusing on addressing the most significant risks first. The results of this risk assessment will inform the development and implementation of security controls.
- Documentation: Document the risk assessment process, findings, and remediation plans.

Given the "low-risk environment" designation, the organization will prioritize readily implementable, cost-effective controls to mitigate identified risks.

3. Data Protection

All PHI and other sensitive data must be protected according to the following standards:

- Data Classification: Data will be classified based on its sensitivity and criticality. PHI will be classified at the highest level of sensitivity.
- Data Encryption: Encryption will be used to protect sensitive data at rest and in transit. Specific encryption standards (e.g., AES-256) will be used as documented in the Organization's Encryption Standard. Data at rest will be encrypted on all laptops, workstations, and servers storing PHI. Data in transit will be encrypted using secure protocols such as HTTPS and VPNs.
- Data Loss Prevention (DLP): Implement preventative measures to prevent unauthorized transmission of PHI outside of approved organization systems. This will include controls such as content filtering and endpoint monitoring where necessary.

- Data Backup and Recovery: Regular backups of critical data will be performed, and backup data will be stored in a secure, off-site location. The Organization will maintain a documented data recovery plan that outlines the steps required to restore data in the event of a disaster or data loss incident. Backups will be tested regularly to ensure their effectiveness.
- Data Minimization: Limit the collection, use, and retention of PHI to the minimum necessary to achieve the intended purpose.
- Data Retention: Establish and adhere to a data retention schedule that defines how long different types of data must be retained and when they should be securely destroyed.
- Data Disposal: Data must be securely disposed of when it is no longer needed. This includes physical destruction of media and secure wiping of electronic storage devices, according to NIST standards (e.g., NIST SP 800-88).

4. Access Controls

Access to PHI and other sensitive data will be restricted to authorized personnel only, based on the principle of least privilege.

- User Accounts: All users must have unique user accounts with strong passwords. Default passwords must be changed immediately upon account creation.
- Password Policy: Passwords must meet minimum complexity requirements (e.g., minimum length, character requirements) and must be changed regularly, at least every 90 days. Password re-use is strictly prohibited.
- Multi-Factor Authentication (MFA): MFA will be implemented for all users accessing sensitive data or systems, especially for remote access and privileged accounts.
- Role-Based Access Control (RBAC): Access to data and systems will be granted based on job roles and responsibilities. Access rights will be reviewed and updated regularly, at least annually.
- Access Revocation: Access to systems and data will be promptly revoked when an employee leaves the organization or changes roles.
- Physical Access: Physical access to data centers and other sensitive areas will be restricted to authorized personnel only. Access control mechanisms, such as key cards or biometric scanners, will be used to control physical access. Visitor access will be logged and monitored.
- Remote Access: All remote access to the Organization's network must be through a secure VPN connection with MFA enabled. Personal devices used for remote access must comply with the Organization's Bring Your Own Device (BYOD) policy (if applicable), including security software and patching requirements.

5. Incident Response

The Organization will maintain a documented Incident Response Plan (IRP) that outlines the steps to be taken in the event of a security incident. The IRP will:

- Define incident types: Clearly define what constitutes a security incident.
- Establish roles and responsibilities: Assign roles and responsibilities to individuals or teams responsible for responding to incidents.
- Outline incident response procedures: Describe the steps to be taken to identify, contain,

eradicate, and recover from security incidents.
- Establish communication protocols: Define how internal and external stakeholders will be notified of security incidents.
- Include forensic analysis procedures: Outline the steps to be taken to preserve evidence and conduct forensic analysis following a security incident.
- Mandatory Reporting: Mandate employees to report suspected and actual security breaches or vulnerabilities through established channels.
- Periodic Testing: The IRP will be tested regularly through tabletop exercises or simulations to ensure its effectiveness. The IRP will be reviewed and updated at least annually, or more frequently if significant changes occur to the IT environment or threat landscape.

6. Security Awareness Training

All employees, contractors, and vendors will receive security awareness training at least annually. Training will cover topics such as:

- Password security: Creating strong passwords, avoiding password reuse, and protecting passwords from phishing attacks.
- Phishing awareness: Identifying and avoiding phishing emails and other social engineering attacks.
- Malware prevention: Avoiding malicious websites and attachments, and reporting suspected malware infections.
- Data protection: Handling PHI and other sensitive data in a secure manner.
- Physical security: Protecting physical assets from theft and unauthorized access.
- Incident reporting: Reporting suspected security incidents to the appropriate personnel.
- Policy Adherence: Understanding the organization's security policies and procedures.

Training will be tailored to the specific roles and responsibilities of individuals.
Records of training completion will be maintained.

7. Compliance and Auditing

The Organization is committed to complying with all applicable laws, regulations, and standards, including NIST cybersecurity framework.

- Regular Audits: Regular internal and external audits will be conducted to assess compliance with this policy and other applicable security standards.
- Vulnerability Scanning: Regular vulnerability scanning will be performed on the Organization's systems and networks to identify potential security weaknesses. Identified vulnerabilities will be promptly remediated.
- Penetration Testing: Periodic penetration testing will be conducted to simulate real-world attacks and identify vulnerabilities that could be exploited by attackers.
- Policy Review: This Cybersecurity Policy will be reviewed and updated at least annually, or more frequently if significant changes occur to the IT environment, business operations, or regulatory landscape.
- Documentation: Maintain comprehensive documentation of security policies, procedures, and controls.

8. Conclusion

This Cybersecurity Policy is essential for protecting the Organization's PHI and other sensitive data. All employees, contractors, and vendors are expected to adhere to this policy. Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract. This policy is a living document and will be updated as needed to reflect changes in the threat landscape and the Organization's business operations. The CISO is responsible for the implementation, maintenance, and enforcement of this policy.