Cybersecurity Policy for Low-Risk Healthcare Environment

1. Introduction

This Cybersecurity Policy outlines the minimum-security standards necessary to protect the confidentiality, integrity, and availability of Protected Health Information (PHI) and other sensitive data held by [Organization Name]. This policy is designed for a low-risk environment, acknowledging limited resources and focusing on fundamental cybersecurity controls. All employees, contractors, vendors, and other individuals or entities accessing or using [Organization Name]'s systems and data must adhere to this policy. The objectives of this policy are to:

- Comply with the Health Insurance Portability and Accountability Act (HIPAA) and other applicable regulations.
- Protect PHI from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Minimize the impact of security incidents.
- Establish a culture of security awareness and responsibility.

2. Risk Assessment

[Organization Name] will conduct a risk assessment at least annually, or more frequently if significant changes occur in the environment (e.g., new systems, regulations), to identify potential threats and vulnerabilities to its information systems and PHI. The risk assessment will be based on the --NIST Cybersecurity Framework (CSF)--, tailored to the organization's size and complexity. The risk assessment will:

- Identify and document assets containing or processing PHI, categorized by criticality and sensitivity. This includes hardware, software, data, and personnel.
- Identify and document potential threats and vulnerabilities that could compromise the confidentiality, integrity, or availability of PHI. This will include but not limited to threats from malware, phishing, ransomware, insider threats, and vulnerabilities in software and hardware.
- Assess the --likelihood-- and --impact-- of identified risks. --Likelihood-- will be assessed using a scale (e.g., Low, Medium, High) based on factors such as the prevalence of the threat, the existence of known vulnerabilities, and the effectiveness of existing controls. --Impact-- will be assessed using a scale (e.g., Low, Medium, High) based on factors such as the number of patients affected, the potential for financial loss, and the potential for reputational damage. Specific criteria for each level (Low, Medium, High) for Likelihood and Impact will be defined and documented in the Risk Assessment Procedure.
- Prioritize risks based on their potential impact and likelihood. Risks will be ranked using a matrix approach, combining likelihood and impact scores.
- Develop and implement mitigation strategies to address identified risks. Mitigation strategies may include:
- --Technical Controls:-- Implementing firewalls, intrusion detection/prevention systems (IDS/IPS), anti-malware software, and data encryption.
- --Administrative Controls:-- Developing and enforcing security policies, conducting security awareness training, and implementing access controls.

- --Physical Controls:-- Securing physical access to facilities and data centers.
- Document the risk assessment process and results, including any identified gaps and remediation plans. The risk assessment report will be reviewed and approved by senior management.

Due to the Low risk environment, the risk assessment will focus on readily available threat intelligence and common vulnerabilities, using standardized frameworks where possible. The assessment will be right-sized to the organization, using questionnaires and interviews to gather information from key stakeholders. A formal penetration test is not required but vulnerability scans should be implemented at least quarterly using a reputable vulnerability scanner (e.g., Nessus Essentials). The vulnerability scans will be reviewed and remediated appropriately.

3. Data Protection

--3.1. Data Encryption:--

All electronic PHI (ePHI) stored at rest on portable devices (e.g., laptops, tablets, USB drives) must be encrypted using a strong encryption algorithm (e.g., AES 256-bit). Encryption of data at rest on servers and workstations is recommended and will be implemented where feasible. Encryption of data in transit over public networks (e.g., the internet) is required, using protocols such as TLS (Transport Layer Security) version 1.2 or higher or VPN (Virtual Private Network) with AES 256-bit encryption.

--3.2. Data Backup and Recovery:--

Regular backups of all critical data, including ePHI, will be performed and stored securely, both on-site (protected from environmental hazards) and off-site (using a secure, reputable cloud backup provider or physical media stored in a secure location). Backup frequency will be determined based on the criticality of the data and the recovery time objective (RTO). A documented data recovery plan will be maintained and tested at least annually to ensure the ability to restore data in the event of a disaster or system failure. Test results will be documented.

--3.3. Data Minimization:--

[Organization Name] will collect and retain only the minimum amount of PHI necessary to fulfill its legitimate business purposes. Data retention policies will be established and followed to ensure that PHI is securely disposed of when it is no longer needed, in accordance with HIPAA guidelines and applicable state laws.

--3.4. Data Loss Prevention (DLP):--

Basic DLP measures will be implemented to prevent the unauthorized transfer of PHI outside of [Organization Name]'s control. This includes:

- --Restricting the use of personal email accounts:-- Employees are prohibited from sending PHI through personal email accounts. Company-provided email accounts should be used for all business communications involving PHI.
- --Restricting the use of unauthorized file-sharing services:-- The use of unsanctioned file-sharing services (e.g., Dropbox, Google Drive) is prohibited for storing or sharing

PHI. Approved, secure file-sharing solutions will be provided and used instead.
- --Monitoring network traffic for unusual activity:-- Basic network monitoring will be implemented to detect unusual data transfer patterns that may indicate data exfiltration. This may involve reviewing network logs and alerts for large file transfers or transfers to unknown destinations.
- --Endpoint monitoring:-- Implementing basic endpoint monitoring to detect attempts to copy PHI to removable media or upload PHI to unauthorized cloud services.
- --Email filtering:-- Implementing email filtering rules to detect and block emails containing PHI being sent to external domains.

--3.5. Media Disposal:--

All electronic media containing PHI must be securely erased using a NIST 800-88 compliant data sanitization method (e.g., overwriting with multiple passes, degaussing) or physically destroyed (e.g., shredding, crushing) before disposal. Documentation of the disposal process, including serial numbers of destroyed devices, will be maintained.

4. Access Controls

--4.1. User Authentication:--

All users must authenticate to access [Organization Name]'s systems and data using strong passwords or multi-factor authentication (MFA) where feasible. Password policies will be enforced, requiring users to create strong passwords that are regularly changed. Strong passwords must:

- Be at least 12 characters in length.
- Contain a mix of uppercase and lowercase letters.
- Contain at least one number.
- Contain at least one special character (e.g., !@#$%^&-).
- Not be based on personal information (e.g., names, birthdates).
- Not be reused within the last 24 passwords.
- Passwords must be changed at least every 90 days.
- Account lockout after 5 failed login attempts for 15 minutes.

Multi-factor authentication (MFA) is required for all users accessing sensitive systems or data, including remote access and access to ePHI.

--4.2. Access Rights Management:--

Access to PHI will be granted on a "need-to-know" basis, using role-based access control (RBAC). Users will only be granted access to the data and systems that they require to perform their job duties. Access rights will be reviewed and updated at least annually, or when an employee's job role changes. A documented procedure for granting, modifying, and revoking access rights will be maintained.

--4.3. Physical Security:--

Physical access to [Organization Name]'s facilities and data centers will be restricted to authorized personnel. Security measures, such as locks, alarms, and surveillance cameras, will be implemented to protect against unauthorized physical access. Visitor access will

be logged and monitored. Data centers will be protected from environmental hazards (e.g., fire, flood).

--4.4. Remote Access:--

Remote access to [Organization Name]'s systems and data will be secured using VPNs with strong encryption (AES 256-bit). Multi-factor authentication (MFA) is required for all remote access connections. Remote access connections will be logged and monitored.

--4.5. Termination of Access:--

Access to [Organization Name]'s systems and data will be promptly revoked (within 24 hours) when an employee or contractor leaves the organization or changes roles. A documented process for terminating access will be followed.

5. Incident Response

--5.1. Incident Reporting:--

All security incidents, including suspected breaches of PHI, must be reported immediately to the designated incident response team (designated contact information provided). Employees are trained to report via phone and email.

--5.2. Incident Response Plan:--

[Organization Name] will maintain a documented incident response plan that outlines the steps to be taken in the event of a security incident. The plan will include procedures for:

- Identifying and containing the incident.
- Assessing the scope and impact of the incident.
- Notifying affected parties, including regulatory agencies (HHS), as required by law (HIPAA Breach Notification Rule). Specific timelines and procedures for notification are included in the plan.
- Remediating the vulnerabilities that led to the incident.
- Documenting the incident and the response.
- Post-incident review and improvement. Lessons learned from each incident will be documented and used to improve the incident response plan and security controls.

The Incident Response Plan will be tested at least annually through tabletop exercises.

--5.3. Breach Notification:--

In the event of a breach of unsecured PHI, [Organization Name] will comply with all applicable breach notification requirements under HIPAA and other relevant regulations. This includes notifying affected individuals, HHS, and, in some cases, the media.

6. Security Awareness Training

--6.1. Training Program:--

All employees, contractors, and other individuals accessing [Organization Name]'s systems and data will receive security awareness training upon hire and annually thereafter. The

training will cover topics such as:

- HIPAA compliance requirements.
- Identifying and avoiding phishing attacks (including real-world examples and simulations).
- Creating strong passwords and password management.
- Protecting PHI from unauthorized access and disclosure (including proper handling of physical documents).
- Reporting security incidents (including contact information for reporting).
- Safe internet and email usage.
- Social engineering awareness (including examples of social engineering tactics).
- Data Loss Prevention (DLP) procedures and policies.
- Mobile device security best practices.

--6.2. Training Records:--

Records of security awareness training will be maintained for all individuals, including the date of training and the topics covered. These records will be reviewed during audits.

7. Compliance and Auditing

--7.1. Compliance Officer:--

A designated Compliance Officer will be responsible for overseeing [Organization Name]'s compliance with HIPAA and other applicable regulations. The Compliance Officer will have the authority and resources necessary to perform their duties.

--7.2. Audits:--

Regular audits will be conducted to assess [Organization Name]'s compliance with this Cybersecurity Policy and relevant regulations. Audits may include:

- Review of security policies and procedures.
- Vulnerability scans and penetration testing (risk-based). Internal vulnerability scans will be conducted quarterly. External penetration testing will be conducted every two years, based on the results of the risk assessment.
- Review of access controls and user permissions.
- Review of incident response procedures.
- Review of security awareness training records.
- Review of data disposal procedures.
- Log reviews and analysis.

--7.3. Corrective Action:--

Any identified compliance gaps or security vulnerabilities will be addressed promptly through corrective action. A formal corrective action plan will be developed and implemented to address any identified findings. The corrective action plan will include timelines for remediation and responsible parties.

8. Conclusion

This Cybersecurity Policy is essential for protecting the confidentiality, integrity, and availability of PHI and other sensitive data held by [Organization Name]. By adhering to

this policy, we can minimize the risk of security incidents and comply with HIPAA and other applicable regulations. This policy will be reviewed and updated at least annually, or as needed to address changes in the threat landscape or regulatory requirements. All personnel are responsible for understanding and adhering to the principles outlined within this document. The policy will be readily available to all employees (e.g., on the company intranet).