Cybersecurity Policy for Healthcare Organizations (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 our organization. This policy is designed for an environment where a documented risk assessment, performed according to section 2, has determined that the overall risk level is low. This assessment considers the organization's size, complexity, data sensitivity, and threat landscape. All employees, contractors, vendors, and other individuals accessing our systems and data are required to adhere to this policy. This policy will be reviewed and updated at least annually, or more frequently as needed, to address evolving threats and changes in the regulatory landscape.

2. Risk Assessment

It is crucial to maintain an understanding of the organization's threat landscape and vulnerabilities, and to validate the "low-risk" environment status.

- Periodic Vulnerability Scans: Conduct regular vulnerability scans of systems and applications, at least quarterly, using automated tools to identify potential weaknesses. Focus should be given to internet-facing services or those directly involved in handling PHI.
- Annual Risk Assessment: Perform a comprehensive risk assessment at least annually to identify potential threats, vulnerabilities, and the likelihood and impact of security incidents. This assessment will consider factors such as the organization's size, complexity, and the nature of the PHI it handles. The Risk Assessment will include an inventory of IT assets and data flows and will be led by the IT Manager. Methodologies such as NIST 800-30 or ISO 27005 may be used as a guide. The risk assessment must, at a minimum, address controls outlined in HIPAA Security Rule 45 CFR § 164.308.
- Risk Mitigation: Implement reasonable and appropriate security controls to mitigate identified risks. This may include technical controls (e.g., patching systems) and administrative controls (e.g., updating policies and procedures). Due to the low risk environment, the focus should be on high impact and low effort mitigations. Examples of potential threats include malware infections, phishing attacks targeting employee credentials, and unauthorized access to patient data.

3. Data Protection

Protecting sensitive data is paramount.

- Data Encryption: Sensitive data, including PHI, should be encrypted at rest and in transit. At a minimum, data at rest must be encrypted using AES 256-bit encryption or a stronger algorithm. Data in transit must be encrypted using TLS 1.2 or a more recent version. Key management procedures must include secure storage, rotation, and access control. All laptops, workstations, and mobile devices that store or access PHI must have full disk encryption enabled.
- Data Loss Prevention (DLP): Implement basic DLP measures to prevent sensitive data from leaving the organization's control. These measures include monitoring email traffic for

sensitive keywords or patterns, restricting the transfer of sensitive files to external storage devices, and preventing the copying of sensitive data to personal email accounts.
- Data Backup and Recovery: Regularly back up critical data, including PHI, to a secure offsite location. Test data recovery procedures at least annually to ensure data can be restored in a timely manner in the event of a disaster or system failure.
- Data Minimization: Only collect and retain PHI that is necessary for legitimate business purposes. Implement data retention policies to securely dispose of data when it is no longer needed.
- Physical Security: Protect physical access to facilities and equipment where sensitive data is stored. This includes implementing access controls, such as locks and security cameras.
- Data Classification: Classify data based on its sensitivity (e.g., Public, Confidential, Restricted). Implement appropriate security controls based on the data classification level.

4. Access Controls

Restrict access to systems and data based on the principle of least privilege.

- User Authentication: Implement strong authentication measures, such as multi-factor authentication (MFA), where feasible, to verify user identities. Enforce strong password policies requiring complex passwords that are changed regularly. Employees must not reuse passwords across personal and work accounts and should utilize password managers where possible.
- Access Management: Grant access to systems and data based on job roles and responsibilities. Regularly review and update user access privileges to ensure they remain appropriate. Implement role-based access controls (RBAC) where possible.
- Account Management: Establish procedures for creating, modifying, and disabling user accounts in a timely manner. Remove access for terminated employees immediately.
- Remote Access: Secure remote access to systems and data using VPNs with strong encryption. Enforce MFA for all remote access connections.
- Privileged Access Management (PAM): Implement controls for privileged accounts, such as limiting the number of users with administrative rights and monitoring privileged account activity.

5. Incident Response

Establish a plan to effectively respond to and recover from security incidents.

- Incident Response Plan (IRP): Develop and maintain a comprehensive Incident Response Plan (IRP) that outlines the procedures for identifying, containing, eradicating, and recovering from security incidents. The IRP will define roles and responsibilities, communication plans, forensic procedures, escalation paths, and containment strategies. The primary stakeholders for incident management are the IT Manager (primary contact), the Practice Manager (communication liaison), and the designated HIPAA Security Officer (compliance oversight). Backups for these roles will be pre-designated and documented within the IRP. Incident management will be facilitated through a dedicated ticketing system or a secure communication platform.

- Incident Reporting: Establish a clear process for reporting suspected security incidents. Encourage employees to report any unusual or suspicious activity immediately.
- Incident Analysis: Investigate security incidents to determine the root cause and implement corrective actions to prevent future incidents.
- Data Breach Notification: Comply with all applicable data breach notification laws and regulations, including HIPAA's Breach Notification Rule. Document and report breaches according to regulatory requirements.
- Regular Testing: Periodically test the Incident Response Plan through tabletop exercises or simulations to ensure its effectiveness.

6. Security Awareness Training

Educate employees about cybersecurity threats and best practices.

- Annual Training: Provide annual security awareness training to all employees, contractors, and vendors who access the organization's systems and data.
- Training Content: Training should cover topics such as phishing awareness, password security, data protection, incident reporting, and social engineering.
- Phishing Simulations: Conduct periodic phishing simulations to test employee awareness and identify areas for improvement.
- Policy Dissemination: Ensure that all employees are aware of and understand the organization's cybersecurity policies and procedures.

7. Compliance and Auditing

Maintain compliance with HIPAA and other applicable regulations.

- HIPAA Compliance: Comply with all applicable HIPAA regulations, including the Privacy Rule, Security Rule, and Breach Notification Rule.
- Regular Audits: Conduct regular internal audits to assess compliance with this policy and other applicable regulations. Engage a qualified external auditor to conduct an independent audit at least every two years.
- Documentation: Maintain thorough documentation of all security policies, procedures, and activities.
- Business Associate Agreements (BAA): Ensure that all business associates have signed Business Associate Agreements (BAAs) that comply with HIPAA requirements. Review and update BAAs annually. Prior to engaging a vendor, conduct due diligence to assess their security posture, including reviewing their security policies and certifications (e.g., SOC 2). Ongoing monitoring of vendor security practices will be performed through periodic questionnaires or audits, as appropriate. Security requirements for vendors will be clearly defined in contracts and BAAs, addressing areas such as data encryption, access controls, and incident response.
- Logging and Monitoring: Implement security monitoring and logging practices. System logs, application logs, and network traffic logs should be enabled and regularly reviewed. Log retention should be at least 90 days. The IT Manager is responsible for reviewing logs and investigating suspicious activity. Specific events to be logged include user logins/logouts, access to sensitive data, and system errors.
- Policy Review: This policy will be reviewed and updated at least annually, or more

frequently as needed, to address evolving threats and changes in the regulatory landscape.

8. Conclusion

This Cybersecurity Policy is essential for protecting our organization's sensitive data and maintaining the trust of our patients. All employees are responsible for adhering to this policy and contributing to a secure environment. While operating in a low-risk environment, consistent vigilance and adherence to these guidelines are critical for safeguarding PHI and ensuring continued compliance. Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract.