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 applies to all employees, contractors, vendors, and other authorized users who access, use, or manage organizational information assets. Given our assessment as a "low risk" environment, the controls outlined herein reflect a proportionate and pragmatic approach to cybersecurity, balancing security needs with operational efficiency and resource constraints. This policy is designed to comply with applicable regulations, including those outlined in ISO/IEC 27001, and demonstrates our commitment to maintaining a secure environment for our patients, partners, and stakeholders.

--2. Risk Assessment--

A formal risk assessment will be conducted annually, or more frequently if significant changes occur in the threat landscape or our operational environment. This assessment will identify potential threats and vulnerabilities to our information assets. Given our classification as a "low risk" environment, the risk assessment will focus on identifying easily exploitable vulnerabilities and common threat vectors, such as phishing attacks and malware infections. The risk assessment methodology will be documented and consistently applied. Identified risks will be documented in a risk register, prioritized based on potential impact and likelihood, and addressed through appropriate mitigation strategies outlined in this policy and supporting procedures.

--3. Data Protection--

- --Data Classification:-- All data will be classified based on its sensitivity and criticality. Data containing PHI will be classified as highly sensitive and will be subject to enhanced protection measures.
- --Data Encryption:-- Encryption will be employed to protect PHI and other sensitive data at rest and in transit. This will include encrypting laptops, storage devices, and email communications. Specific encryption technologies will be selected based on industry best practices and cost-effectiveness.
- --Data Backup and Recovery:-- Regular backups of critical data, including PHI, will be performed and stored securely in an offsite location. Backup procedures will be tested periodically to ensure data can be recovered in a timely manner. A documented data recovery plan will be maintained and tested regularly.
- --Data Loss Prevention (DLP):-- Controls will be implemented to prevent unauthorized disclosure of PHI and other sensitive data. These controls may include monitoring network traffic for sensitive data leaving the organization, implementing restrictions on removable media, and educating employees about proper data handling procedures.
- --Data Retention and Disposal:-- Data will be retained only as long as required by law or business necessity. Data will be disposed of securely using methods that prevent

unauthorized access, such as data wiping or physical destruction of storage media.

--4. Access Controls--

- --Principle of Least Privilege:-- Access to information assets will be granted based on the principle of least privilege, meaning users will only be granted access to the information and systems they need to perform their job duties.
- --User Account Management:-- User accounts will be created, managed, and terminated in a timely manner. Strong passwords will be enforced, and multi-factor authentication (MFA) will be implemented where feasible, particularly for access to sensitive systems and data.
- --Access Control Lists (ACLs):-- Access to files, folders, and systems will be controlled through ACLs, which specify which users or groups have access to specific resources. ACLs will be reviewed regularly to ensure they are accurate and up-to-date.
- --Remote Access:-- Remote access to organizational systems will be secured using VPNs or other secure methods. Multi-factor authentication will be required for all remote access connections.
- --Physical Security:-- Physical access to data centers and other sensitive areas will be restricted to authorized personnel only. Access will be controlled through physical access controls, such as keycards or biometric scanners.

--5. Incident Response--

- --Incident Response Plan:-- A documented incident response plan will be maintained and tested regularly. The plan will outline the steps to be taken in the event of a security incident, including roles and responsibilities, communication protocols, and escalation procedures.
- --Incident Reporting:-- All suspected security incidents will be reported to the designated incident response team immediately.
- --Incident Analysis:-- Security incidents will be thoroughly analyzed to determine the root cause and impact. Lessons learned from incident analysis will be used to improve security controls and incident response procedures.
- --Incident Containment and Eradication:-- Measures will be taken to contain and eradicate security incidents as quickly as possible. This may include isolating affected systems, removing malware, and restoring data from backups.
- --Post-Incident Activity:-- Following an incident, a post-incident review will be conducted to assess the effectiveness of the incident response and identify areas for improvement.

--6. Security Awareness Training--

- --Employee Training:-- All employees will receive security awareness training upon hire and annually thereafter. Training will cover topics such as phishing awareness, password security, data handling procedures, and incident reporting.
- --Phishing Simulations:-- Periodic phishing simulations will be conducted to test

employees' awareness of phishing attacks and identify areas where additional training is needed.

- --Security Awareness Communications:-- Regular security awareness communications, such as newsletters and posters, will be distributed to employees to reinforce security best practices.

--7. Compliance and Auditing--

- --ISO/IEC 27001 Compliance:-- This policy is aligned with the principles and guidelines of ISO/IEC 27001. The organization will maintain documentation demonstrating compliance with this standard.
- --Regular Audits:-- Internal audits will be conducted at least annually to assess the effectiveness of security controls and compliance with this policy. External audits may also be conducted periodically to provide independent assurance of our security posture.
- --Policy Review:-- This policy will be reviewed and updated at least annually, or more frequently if necessary, to reflect changes in the threat landscape, regulatory requirements, or organizational operations.

--8. Conclusion--

This Cybersecurity Policy represents our organization's commitment to protecting the confidentiality, integrity, and availability of our information assets. By adhering to this policy and supporting procedures, we can minimize our risk exposure, maintain compliance with applicable regulations, and ensure the continued trust of our patients, partners, and stakeholders. All members of the organization are expected to understand and comply with this policy. Violations of this policy may result in disciplinary action, up to and including termination of employment or contract.