# Cybersecurity Policy for Healthcare Organizations (Low Risk Environment)

### 1. Introduction

This Cybersecurity Policy outlines the mandatory requirements for protecting the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI) and other sensitive data within [Organization Name]. This policy applies to all employees, contractors, vendors, and any other individuals or entities accessing or using [Organization Name]'s information systems and data. This policy acknowledges that [Organization Name] currently operates in a low-risk environment, characterized by limited external connectivity, a small user base with clearly defined roles, and a focus on established, well-maintained systems. While considered low-risk, adherence to this policy is critical for maintaining that risk profile and complying with relevant regulations, including the Risk Management Framework (RMF). Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.

### 2. Risk Assessment

[Organization Name] recognizes the importance of proactively identifying and managing cybersecurity risks. Although we operate in a low-risk environment, periodic risk assessments are essential.

- --Frequency:-- Risk assessments will be conducted at least annually, and more frequently if significant changes occur to the IT infrastructure, business operations, or threat landscape.
- --Methodology:-- Risk assessments will be conducted using a standardized methodology consistent with NIST Special Publication 800-30, "Guide for Conducting Risk Assessments." This includes identifying assets, threats, vulnerabilities, likelihood, and impact.
- --Scope:-- Assessments will encompass all systems and data that store, process, or transmit ePHI and other sensitive information.
- --Documentation:-- Risk assessment findings will be documented in a formal risk register, which will include prioritized risks and planned mitigation strategies.
- --Management Review:-- The risk register will be reviewed and approved by senior management.

### 3. Data Protection

Protecting data is paramount. This section outlines the requirements for data protection at rest and in transit.

- --Data Encryption:-- ePHI and other sensitive data stored on servers, workstations, and portable devices must be encrypted using strong encryption algorithms (e.g., AES-256).
- --Data Loss Prevention (DLP):-- DLP measures will be implemented to prevent sensitive data from leaving the organization's control without authorization. This may include monitoring email communications, network traffic, and removable media usage.
- --Data Backup and Recovery:-- Regular backups of all critical data will be performed and stored securely in an offsite location. Backup and recovery procedures will be tested regularly to ensure data can be restored in a timely manner in the event of a disaster.
- --Data Sanitization:-- When disposing of hardware or storage media, all data must be

securely sanitized using industry-standard methods (e.g., DoD 5220.22-M).
- --Data Minimization:-- Only collect and retain data that is necessary for legitimate business purposes. Periodically review data retention policies and delete data that is no longer needed.

### 4. Access Controls

Limiting access to sensitive data is critical to prevent unauthorized disclosure.

- --Principle of Least Privilege:-- Access to systems and data will be granted based on the principle of least privilege, meaning that users will only be granted the minimum level of access required to perform their job duties.
- --User Account Management:--
- Unique user accounts will be created for each individual accessing the organization's systems.
- Default passwords must be changed immediately upon account creation.
- User accounts will be disabled promptly when an employee or contractor leaves the organization or changes roles.
- Regular audits of user accounts will be conducted to ensure that access privileges are appropriate.
- --Password Management:--
- Strong passwords must be used, adhering to complexity requirements (e.g., minimum length, mixed case, special characters).
- Passwords must be changed at least every 90 days.
- Password reuse is prohibited.
- Multi-factor authentication (MFA) should be implemented where feasible, especially for privileged accounts and remote access.
- --Access Logging and Monitoring:-- All access to sensitive systems and data will be logged and monitored for suspicious activity. Logs will be reviewed regularly.
- --Physical Security:-- Physical access to servers and other critical infrastructure will be restricted to authorized personnel only.

### 5. Incident Response

Even in a low-risk environment, security incidents can occur. A well-defined incident response plan is essential.

- --Incident Response Plan (IRP):-- A written IRP will be maintained and regularly updated. The IRP will outline the steps to be taken in the event of a security incident, including identification, containment, eradication, recovery, and lessons learned.
- --Incident Reporting:-- All suspected security incidents must be reported immediately to the designated Incident Response Team (IRT).
- --Incident Handling Procedures:-- The IRT will follow established procedures for investigating and resolving security incidents.
- --Communication Plan:-- The IRP will include a communication plan for notifying stakeholders of security incidents, as appropriate.
- --Post-Incident Review:-- After each security incident, a post-incident review will be conducted to identify the root cause of the incident and to improve security controls.

- --Regular Testing:-- The IRP will be tested regularly through tabletop exercises and simulations.

### 6. Security Awareness Training

Security awareness training is crucial to educate users about cybersecurity risks and best practices.

- --Initial Training:-- All new employees and contractors will receive security awareness training upon hire.
- --Annual Training:-- All employees and contractors will receive annual security awareness training.
- --Training Content:-- Training will cover topics such as:
- Password security
- Phishing awareness
- Social engineering
- Malware prevention
- Data protection
- Incident reporting
- Acceptable use of technology
- --Training Delivery:-- Training will be delivered through a variety of methods, such as online modules, instructor-led sessions, and phishing simulations.
- --Training Records:-- Records of all security awareness training will be maintained.

### 7. Compliance and Auditing

[Organization Name] is committed to complying with all applicable laws, regulations, and standards, including the Risk Management Framework (RMF).

- --RMF Alignment:-- This policy is designed to align with the RMF, focusing on the essential security controls appropriate for a low-risk environment. Specific controls from NIST SP 800-53 Revision 5 will be selected and implemented based on the results of risk assessments.
- --Regular Audits:-- Internal and external audits will be conducted regularly to assess compliance with this policy and other relevant regulations.
- --Vulnerability Scanning:-- Regular vulnerability scans will be performed on all systems to identify and remediate security vulnerabilities.
- --Penetration Testing:-- Penetration testing will be conducted periodically to assess the effectiveness of security controls.
- --Compliance Reporting:-- Regular reports on compliance with this policy and other relevant regulations will be provided to senior management.
- --Policy Review:-- This policy will be reviewed and updated at least annually, or more frequently if necessary, to reflect changes in the business environment, threat landscape, or regulatory requirements.

### 8. Conclusion

This Cybersecurity Policy is a living document that will be continuously improved and updated to reflect the evolving threat landscape and the changing needs of [Organization

Name]. By adhering to this policy, we can protect our patients' data, maintain the integrity of our systems, and ensure the continued success of our organization. All personnel are responsible for understanding and complying with the requirements outlined in this policy. Any questions or concerns regarding this policy should be directed to the Information Security Officer.