Cybersecurity Policy for Healthcare Organizations (Low Risk Environment)

1. Introduction

This Cybersecurity Policy outlines the minimum security requirements for protecting the confidentiality, integrity, and availability of Protected Health Information (PHI) and other sensitive data within this healthcare organization. This policy applies to all employees, contractors, vendors, and any other individuals or entities accessing or using the organization's information systems, regardless of location or device. While this policy is tailored for a low-risk environment, it is imperative to adhere to its principles to minimize potential harm and maintain compliance with applicable regulations, including those outlined by NIST. This policy is a living document and will be reviewed and updated periodically to reflect changes in the threat landscape, regulatory requirements, and organizational needs.

2. Risk Assessment

This organization conducts a periodic risk assessment to identify, analyze, and evaluate potential threats and vulnerabilities that could compromise the confidentiality, integrity, or availability of its data. While operating in a low-risk environment, the assessment focuses on readily identifiable threats and common vulnerabilities. This includes:

- --Threat Identification:-- Identifying potential sources of harm, such as malware infections, phishing attacks, unauthorized access attempts, and accidental data loss.
- --Vulnerability Assessment:-- Evaluating weaknesses in systems, applications, and processes that could be exploited by identified threats.
- --Risk Analysis:-- Determining the likelihood and impact of potential security incidents. In a low-risk environment, the focus is on mitigating the impact of common vulnerabilities through preventative measures.
- --Risk Mitigation:-- Implementing appropriate security controls to reduce identified risks to an acceptable level. This policy outlines the specific controls mandated within this organization.
- --Regular Review:-- The risk assessment is reviewed and updated at least annually, or more frequently if there are significant changes to the organization's environment, such as the introduction of new technologies or changes in regulatory requirements.

3. Data Protection

Protecting sensitive data, especially PHI, is paramount. The following measures are in place:

- --Data Classification:-- Data is classified based on its sensitivity and criticality. PHI and other confidential information are classified as highly sensitive and require the highest level of protection.
- --Data Encryption:-- Sensitive data, both in transit and at rest, must be encrypted using industry-standard encryption algorithms. This includes data stored on laptops, removable media, and cloud storage services. Data transmission over public networks must utilize secure protocols such as HTTPS or VPNs.

- --Data Loss Prevention (DLP):-- While not always a requirement for low-risk environments, basic DLP principles will be enforced to prevent sensitive data from leaving the organization's control. This includes policies regarding the use of removable media and the transmission of sensitive data via email.
- --Data Backup and Recovery:-- Regular backups of critical data are performed and stored securely in an offsite location. Backup and recovery procedures are tested regularly to ensure data can be restored in a timely manner in the event of a disaster or data loss incident.

4. Access Controls

Access to systems and data is restricted based on the principle of least privilege. This means users are granted only the minimum level of access necessary to perform their job duties.

- --User Authentication:-- All users must authenticate to access the organization's systems and applications using strong passwords and, where possible, multi-factor authentication (MFA). Passwords must meet complexity requirements and be changed regularly.
- --Access Control Lists (ACLs):-- Access to files, folders, and applications is controlled through ACLs. Access permissions are reviewed regularly to ensure they are appropriate and up-to-date.
- --Remote Access:-- Remote access to the organization's network is permitted only through secure channels, such as VPNs. Remote access connections must be authenticated using strong passwords and, where possible, MFA.
- --Account Management:-- User accounts are created, modified, and disabled in a timely manner based on employee onboarding, transfers, and terminations. Regular audits of user accounts are conducted to ensure accuracy and identify any unauthorized accounts.
- --Physical Access:-- Physical access to server rooms and other sensitive areas is restricted to authorized personnel only. Access is controlled through physical access controls, such as key cards or biometric scanners.

5. Incident Response

The organization maintains an Incident Response Plan (IRP) to effectively detect, respond to, and recover from security incidents. The IRP outlines the roles and responsibilities of the incident response team, as well as the procedures for reporting, investigating, and containing security incidents.

- --Incident Reporting:-- All suspected security incidents must be reported immediately to the designated incident response team.
- --Incident Investigation:-- The incident response team will investigate reported incidents to determine the scope and impact of the incident.
- --Incident Containment:-- Measures will be taken to contain the incident and prevent further damage.
- --Incident Eradication:-- The root cause of the incident will be identified and eradicated.
- --Incident Recovery:-- Systems and data will be restored to their normal operating state.
- --Post-Incident Activity:-- A post-incident review will be conducted to identify lessons

learned and improve the organization's security posture.
- --Communication:-- Communication protocols are established to ensure timely and accurate information sharing with relevant stakeholders during an incident.

6. Security Awareness Training

All employees and contractors are required to participate in regular security awareness training. The training covers topics such as:

- --Password Security:-- Creating strong passwords and protecting them from unauthorized access.
- --Phishing Awareness:-- Identifying and avoiding phishing attacks.
- --Malware Prevention:-- Preventing malware infections.
- --Data Protection:-- Protecting sensitive data.
- --Incident Reporting:-- Reporting suspected security incidents.
- --Social Engineering:-- Recognizing and avoiding social engineering attacks.
- --Acceptable Use Policy:-- Understanding and adhering to the organization's acceptable use policy.

The training is tailored to the specific roles and responsibilities of employees. The effectiveness of the training is evaluated through quizzes, surveys, and simulated phishing attacks.

7. Compliance and Auditing

This Cybersecurity Policy is designed to align with relevant compliance standards, including NIST.

- --NIST Framework:-- This policy leverages the NIST Cybersecurity Framework (CSF) to establish a comprehensive cybersecurity program. The five core functions of the CSF (Identify, Protect, Detect, Respond, and Recover) are addressed within this policy.
- --Regular Audits:-- Internal and external audits are conducted regularly to assess compliance with this policy and applicable regulations.
- --Policy Updates:-- This policy will be reviewed and updated at least annually, or more frequently if there are significant changes to the organization's environment or regulatory requirements.
- --Documentation:-- Detailed documentation of security policies, procedures, and controls is maintained and made available to authorized personnel.

8. Conclusion

This Cybersecurity Policy is essential for protecting the organization's information assets and maintaining the trust of patients and stakeholders. All individuals and entities accessing or using the organization's information systems are responsible for adhering 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 provides a baseline for security in a low-risk environment; continuous improvement and adaptation are essential to maintain an effective security posture.