Cybersecurity Policy for Healthcare (Low Risk Environment)

1. Introduction

This Cybersecurity Policy outlines the requirements and guidelines for maintaining 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 any other individuals or entities accessing or using our information systems and data. This policy is designed to address the unique security needs of a low-risk healthcare environment while adhering to the requirements stipulated under DDRO compliance standards. This policy will be reviewed and updated at least annually, or more frequently as needed to address emerging threats and changes in regulations.

2. Risk Assessment

A formal risk assessment will be conducted at least annually to identify, analyze, and evaluate potential threats and vulnerabilities to our information systems and data. The scope of the risk assessment will include:

- --Asset Identification:-- Identification of all physical and logical assets, including hardware, software, data, and facilities.
- --Threat Identification:-- Identification of potential threats, such as malware, phishing attacks, insider threats, and natural disasters.
- --Vulnerability Assessment:-- Assessment of existing vulnerabilities in our systems and processes.
- --Risk Analysis:-- Analysis of the likelihood and impact of each identified threat and vulnerability.
- --Risk Evaluation:-- Evaluation of the overall risk level for each asset and the organization as a whole.
- --Risk Treatment:-- Implementing appropriate security controls to mitigate identified risks based on a risk-based approach.

Due to the "Low Risk" categorization, we will prioritize addressing critical and high-risk vulnerabilities first, but this does not mean that other vulnerability classes will be ignored. Regular scanning and vulnerability assessment will be performed to identify and categorize risks.

3. Data Protection

Protecting sensitive data is paramount. The following data protection measures will be implemented:

- --Data Minimization:-- Limiting the collection, use, and retention of PHI and other sensitive data to only what is necessary for legitimate business purposes.
- --Data Encryption:-- Encrypting sensitive data at rest and in transit using industry-standard encryption algorithms.
- --Data Backup and Recovery:-- Regularly backing up data to secure, offsite locations, and testing the recovery process to ensure data can be restored in the event of a disaster.
- --Data Loss Prevention (DLP):-- Implementing DLP measures to prevent sensitive data from leaving the organization's control. This may include monitoring network traffic, email

communications, and file transfers.

- --Data Retention and Disposal:-- Establishing a data retention schedule and securely disposing of data that is no longer needed in accordance with legal and regulatory requirements.
- --Physical Security:-- Securely storing physical records containing PHI and limiting access to authorized personnel only.

4. Access Controls

Access to information systems and data will be restricted to authorized personnel based on the principle of least privilege. The following access control measures will be implemented:

- --User Authentication:-- Requiring strong passwords and multi-factor authentication (MFA) for all users accessing sensitive systems and data.
- --Role-Based Access Control (RBAC):-- Assigning access rights based on job roles and responsibilities.
- --Access Review:-- Conducting regular access reviews to ensure that users only have the access they need.
- --Privileged Access Management (PAM):-- Implementing PAM controls to manage and monitor privileged accounts.
- --Account Management:-- Establishing procedures for creating, modifying, and disabling user accounts in a timely manner.
- --Physical Access Controls:-- Controlling physical access to facilities and data centers through measures such as security badges, access logs, and surveillance cameras.

5. Incident Response

A comprehensive incident response plan will be maintained to address security incidents in a timely and effective manner. The plan will include:

- --Incident Detection:-- Monitoring systems and networks for suspicious activity and potential security incidents.
- --Incident Reporting:-- Establishing a clear process for reporting security incidents.
- --Incident Response Team:-- Designating an incident response team with clearly defined roles and responsibilities.
- --Incident Containment:-- Implementing measures to contain the impact of a security incident.
- --Incident Eradication:-- Removing the cause of a security incident.
- --Incident Recovery:-- Restoring systems and data to normal operations.
- --Post-Incident Analysis:-- Conducting a post-incident analysis to identify the root cause of the incident and improve security controls.

All employees are responsible for reporting any suspected security incidents immediately to the designated incident response team.

6. Security Awareness Training

All employees, contractors, and vendors will receive security awareness training on an annual basis, or more frequently as needed. The training will cover topics such as:

- --Password Security:-- Creating strong passwords and protecting them from compromise.
- --Phishing Awareness:-- Identifying and avoiding phishing attacks.
- --Malware Awareness:-- Preventing malware infections.
- --Data Protection:-- Protecting sensitive data from unauthorized access and disclosure.
- --Social Engineering:-- Recognizing and avoiding social engineering attacks.
- --Incident Reporting:-- Reporting security incidents promptly.
- --Policy Compliance:-- Understanding and complying with this Cybersecurity Policy.

The training will be tailored to the specific roles and responsibilities of individuals.

7. Compliance and Auditing

This Cybersecurity Policy is designed to comply with DDRO compliance standards, as well as other applicable laws and regulations. Regular audits will be conducted to assess compliance with this policy and to identify areas for improvement.

- --Internal Audits:-- Conducting internal audits on a regular basis.
- --External Audits:-- Engaging external auditors to conduct independent audits.
- --Compliance Monitoring:-- Continuously monitoring compliance with applicable laws and regulations.
- --Policy Enforcement:-- Enforcing this Cybersecurity Policy through appropriate disciplinary measures.
- --Documentation:-- Maintaining accurate and up-to-date documentation of all security policies, procedures, and controls.

8. Conclusion

This Cybersecurity Policy is essential for protecting the confidentiality, integrity, and availability of PHI and other sensitive data within our organization. By adhering to this policy, we can mitigate risks, comply with applicable laws and regulations, and maintain the trust of our patients and stakeholders. All employees, contractors, and vendors are expected to comply with this policy and to actively participate in our cybersecurity efforts. Continued commitment and vigilance are necessary to safeguard our information assets and ensure the security of our healthcare operations.