Cybersecurity Policy for Healthcare Organizations (Low Risk Environment)

1. Introduction

This Cybersecurity Policy outlines the framework for protecting the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI) and other sensitive data within our healthcare organization. This policy is designed to ensure compliance with applicable laws, regulations, and industry best practices, specifically the Risk Management Framework (RMF), while acknowledging the organization's classification as operating in a "low-risk" environment. This classification is based on a documented risk assessment, considering factors such as the volume and sensitivity of data handled, the complexity of IT infrastructure, and the identified threat landscape. All employees, contractors, vendors, and other authorized users are required to adhere to this policy.

2. Risk Assessment

A comprehensive risk assessment will be conducted at least annually, or more frequently if significant changes occur to the organization's environment, such as the introduction of new systems or technologies, or changes to regulations. The risk assessment will:

- --Identify assets:-- Catalog all IT assets, including hardware, software, and data repositories, that store, process, or transmit ePHI or other sensitive information.
- --Identify threats:-- Recognize potential threats to these assets, including but not limited to malware, phishing attacks, unauthorized access, and data breaches.
- --Identify vulnerabilities:-- Assess existing vulnerabilities in systems, applications, and processes that could be exploited by identified threats.
- --Analyze risks:-- Evaluate the likelihood and impact of identified threats exploiting vulnerabilities, considering the potential business consequences.
- --Determine risk level:-- Prioritize risks based on their severity and likelihood, focusing on those that pose the greatest threat to the organization's operations and reputation.

Risk assessment results will be documented and used to inform the development and implementation of appropriate security controls. This policy will be reviewed and updated based on the risk assessment findings.

3. Data Protection

Data protection measures are essential for safeguarding ePHI and other sensitive data. The following principles will be applied:

- --Data Minimization:-- Collect and retain only the minimum necessary data required to fulfill business and legal obligations.
- --Data Encryption:-- Implement encryption for ePHI and other sensitive data both in transit and at rest, using industry-standard encryption algorithms. Encryption keys will be securely managed and protected.
- --Data Backup and Recovery:-- Regularly back up critical data to secure, offsite locations. Test backup and recovery procedures periodically to ensure data can be restored in a timely manner in the event of a system failure or disaster.
- --Data Loss Prevention (DLP):-- Implement DLP measures to prevent the unauthorized

transmission or disclosure of ePHI and other sensitive data. These measures may include content filtering, data masking, and monitoring of data flows.
- --Data Disposal:-- Securely dispose of data and storage media when they are no longer needed, using methods that prevent unauthorized access to the data. Approved methods include physical destruction, data wiping, and degaussing.

4. Access Controls

Access to ePHI and other sensitive data will be restricted to authorized personnel based on the principle of least privilege.

- --User Authentication:-- Implement strong authentication mechanisms, such as multi-factor authentication (MFA) where feasible, to verify the identity of users accessing systems and data.
- --Access Control Lists (ACLs):-- Utilize ACLs to restrict access to specific files, folders, and applications based on user roles and responsibilities.
- --Role-Based Access Control (RBAC):-- Implement RBAC to assign permissions based on job functions, ensuring that users only have access to the data and resources they need to perform their duties.
- --Regular Access Reviews:-- Conduct periodic reviews of user access rights to ensure that they remain appropriate and aligned with current job responsibilities.
- --Account Management:-- Implement procedures for creating, modifying, and disabling user accounts in a timely manner, including when employees leave the organization or change roles.
- --Password Policy:-- Enforce a strong password policy that requires users to create complex passwords, change them regularly, and protect them from unauthorized access.

5. Incident Response

A well-defined incident response plan is crucial for handling security incidents and breaches effectively.

- --Incident Detection:-- Implement monitoring and alerting systems to detect potential security incidents.
- --Incident Reporting:-- Establish clear procedures for reporting suspected security incidents to the designated incident response team.
- --Incident Analysis:-- Conduct thorough investigations to determine the scope and impact of security incidents.
- --Incident Containment:-- Take immediate steps to contain security incidents and prevent further damage.
- --Incident Eradication:-- Remove the root cause of security incidents and restore affected systems to a secure state.
- --Incident Recovery:-- Restore data and systems to their pre-incident state.
- --Post-Incident Activity:-- Document lessons learned from security incidents and update security policies and procedures accordingly.
- --Breach Notification:-- Comply with all applicable breach notification requirements, including those under HIPAA and other relevant regulations.

6. Security Awareness Training

Security awareness training is essential for educating employees and other authorized users about cybersecurity threats and best practices.

- --Initial Training:-- Provide initial security awareness training to all new employees and other authorized users.
- --Ongoing Training:-- Conduct regular security awareness training to reinforce key concepts and address emerging threats. Training should include topics such as:
- Phishing awareness
- Password security
- Data protection
- Social engineering
- Incident reporting
- --Phishing Simulations:-- Conduct periodic phishing simulations to test employees' ability to identify and avoid phishing attacks.
- --Training Records:-- Maintain records of security awareness training for all employees and other authorized users.

7. Compliance and Auditing

Compliance with applicable laws, regulations, and industry standards is a critical aspect of cybersecurity.

- --RMF Implementation:-- The organization will implement controls based on the Risk Management Framework (RMF) as tailored to our low-risk environment. This includes selecting, implementing, assessing, and monitoring security controls as defined by the RMF.
- --Regular Audits:-- Conduct regular internal audits and external assessments to verify compliance with applicable regulations and security policies.
- --Vulnerability Scanning:-- Perform regular vulnerability scans of systems and applications to identify and remediate security vulnerabilities.
- --Penetration Testing:-- Conduct periodic penetration testing to simulate real-world attacks and identify weaknesses in the organization's security posture.
- --Documentation:-- Maintain comprehensive documentation of security policies, procedures, and controls.
- --Compliance Reporting:-- Prepare regular reports on compliance status for management and other stakeholders.

8. Conclusion

This Cybersecurity Policy provides a framework for protecting ePHI and other sensitive data in a low-risk environment within the healthcare industry, aligned with RMF guidelines. All personnel are responsible for understanding and adhering to this policy. The CISO is responsible for overseeing the implementation and enforcement of this policy, and for ensuring that it is reviewed and updated regularly to reflect changes in the threat landscape, business operations, and regulatory requirements. Continuous improvement of security practices is essential to maintaining a strong cybersecurity posture and protecting the organization's assets and reputation.