Cybersecurity Policy for Low-Risk Healthcare Environments

Version: 1.0

Date Issued: October 26, 2023

Effective Date: November 26, 2023

Policy Owner: [Your Name], CISO

1. Introduction

This Cybersecurity Policy outlines the minimum security requirements and guidelines for pr
the confidentiality, integrity, and availability of Protected Health Information (PHI) and othe
sensitive data within this organization. This policy is specifically tailored for environments
categorized as "Low Risk," meaning they handle a limited volume of PHI, utilize primarily cl
based services with built-in security features, and have a restricted number of users access
sensitive data. This policy is aligned with the ISO/IEC 27001 standard and serves as a found
for establishing and maintaining a secure operating environment. All employees, contractor
other individuals with access to organizational information systems are required to adhere
policy.

2. Risk Assessment

While classified as a Low Risk environment, periodic risk assessments are still crucial.

* **Frequency:** Risk assessments will be conducted at least annually or whenever signifi
changes occur within the organization's IT infrastructure, business processes, or regulatory
landscape.
* **Scope:** The risk assessment will identify potential threats and vulnerabilities to
information assets, considering factors such as data storage locations, access controls, and
software applications.
* **Methodology:** A simplified risk assessment methodology will be employed, focusing o
identifying and prioritizing risks based on their potential impact and likelihood of occurrenc
This may involve using a qualitative approach, such as a risk matrix, to categorize risks (e.g
low, medium, high).

*   **Documentation:** Risk assessment findings, including identified risks, their potential i
and implemented mitigation measures, will be documented and reviewed by management.
*   **Mitigation:** Identified risks will be addressed through the implementation of appropri
security controls, as outlined in this policy.

3. Data Protection

Data protection is paramount to maintaining patient privacy and regulatory compliance.

*   **Data Classification:** Data will be classified according to its sensitivity (e.g., public,
internal, confidential). PHI is considered "Confidential" and must be protected accordingly.
*   **Data Encryption:** While not mandatory for all data at rest, encryption is strongly
recommended for storing PHI on laptops, removable media, and within cloud storage servic
Encryption should be considered a default for data in transit, especially when transferring P
outside of the organization's network. Strong encryption algorithms, such as AES-256, shou
where implemented.
*   **Data Backup and Recovery:** Regular backups of critical data, including PHI, will be
performed. Backup frequency will be determined based on the criticality of the data and re
time objectives. Backups will be stored in a secure offsite location or within a resilient cloud
based backup service. Recovery procedures will be documented and tested periodically to
can be restored in a timely manner.
*   **Data Disposal:** When data is no longer needed, it must be disposed of securely. Phys
media (e.g., hard drives, USB drives) must be physically destroyed. Electronic data must be
wiped using industry-standard data sanitization methods.
*   **Third-Party Data Handling:** Any third-party vendors handling PHI must adhere to a Bu
Associate Agreement (BAA) and demonstrate their commitment to data security and privac

4. Access Controls

Access to information systems and data will be restricted based on the principle of least pri
*   **User Account Management:** Each user will be assigned a unique username and passw
accessing organizational systems. Generic or shared accounts are prohibited.

*   **Password Policy:** Users are required to create strong passwords that meet the follow
criteria:
    *   Minimum length of 8 characters
    *   Combination of uppercase and lowercase letters, numbers, and symbols
    *   Passwords must be changed at least every 90 days.
    *   Password reuse is prohibited.
*   **Multi-Factor Authentication (MFA):** MFA is strongly recommended for all users acces
sensitive systems, particularly those containing PHI, especially remotely.
*   **Access Reviews:** User access privileges will be reviewed at least annually to ensure t
appropriate for their current role.
*   **Termination Procedures:** Upon termination of employment, user accounts will be pro
disabled and access privileges revoked.

5. Incident Response

A defined incident response plan is crucial to minimizing the impact of security incidents.

*   **Incident Reporting:** All suspected security incidents, including data breaches, malwa
infections, and unauthorized access attempts, must be reported immediately to the design
security contact (e.g., IT Manager, Security Officer).
*   **Incident Response Plan:** A simplified incident response plan will be maintained, outli
the steps to be taken in the event of a security incident. This plan will include:
    *   Identification and containment of the incident
    *   Eradication of the threat
    *   Recovery of affected systems and data
    *   Post-incident analysis and reporting.
*   **Incident Documentation:** All security incidents will be documented, including the dat
nature of the incident, impact, and remediation steps taken.
*   **Notification Requirements:** In the event of a data breach involving PHI, notification
requirements under applicable regulations (e.g., HIPAA) will be followed.

6. Security Awareness Training

Regular security awareness training is essential for educating users about cybersecurity thr
best practices.

* **Training Frequency:** Security awareness training will be provided to all employees ar
contractors at least annually and upon onboarding.
* **Training Content:** Training will cover topics such as:
  * Password security best practices
  * Phishing awareness and prevention
  * Data protection and privacy
  * Malware prevention
  * Social engineering
  * Incident reporting procedures.
* **Training Delivery:** Training can be delivered through various methods, including onli
modules, in-person presentations, and simulated phishing exercises.
* **Training Documentation:** Employee completion of security awareness training will be
and documented.

7. Compliance and Auditing

Compliance with this policy and applicable regulations will be monitored through regular au
reviews.

* **Policy Review:** This policy will be reviewed and updated at least annually or whenever
significant changes occur in the organization's IT environment, business processes, or regu
landscape.
* **Internal Audits:** Periodic internal audits will be conducted to assess compliance with
policy and identify any gaps in security controls.
* **External Audits:** The organization may be subject to external audits by regulatory bo
third-party assessors to verify compliance with applicable regulations, such as HIPAA, and s
standards, such as ISO/IEC 27001.

*   **Compliance Reporting:** The results of audits and reviews will be documented and re

management.

8. Conclusion

This Cybersecurity Policy provides a framework for protecting the confidentiality, integrity,

availability of information assets in a Low Risk healthcare environment. Adherence to this

is mandatory for all individuals with access to organizational systems and data. By impleme

these security controls and promoting a culture of security awareness, we can mitigate risk

protect patient privacy, and ensure compliance with applicable regulations. This policy is a

document and will be continuously improved to address evolving threats and maintain a st

security posture.