Cybersecurity Policy for Low-Risk Healthcare Environment

Version: 1.0

Effective Date: October 26, 2023

Applicability: This policy applies to all employees, contractors, volunteers, and any other individuals or entities accessing, processing, or storing Protected Health Information (PHI) and Personally Identifiable Information (PII) within this low-risk healthcare environment.

1. Introduction

This Cybersecurity Policy outlines the minimum security requirements for protecting the confidentiality, integrity, and availability of Protected Health Information (PHI) and Personally Identifiable Information (PII) within this low-risk healthcare environment. This policy is designed to be proportionate to the identified risks and aligned with applicable regulations, including the General Data Protection Regulation (GDPR).

This environment is characterized as low-risk based on the following factors (but not limited to):

- Limited number of patients served.
- Minimal use of digital health records or primarily paper-based systems.
- Limited or no electronic billing or insurance claims processing.
- No public-facing websites or online portals containing PHI.
- Low volume of PHI processed.

This policy will be reviewed and updated at least annually or more frequently as required by changes in the threat landscape, regulatory requirements, or business operations. All personnel are responsible for understanding and adhering to this policy.

2. Risk Assessment

A risk assessment, proportionate to the low-risk environment, will be conducted annually to identify potential threats and vulnerabilities to PHI and PII. This assessment will consider:

- Potential threats to data confidentiality, integrity, and availability (e.g., malware, phis
- Vulnerabilities in systems and processes (e.g., weak passwords, outdated software, la
- The likelihood and potential impact of identified risks.

The risk assessment will be used to prioritize security controls and inform decision-making regarding resource allocation. Documentation of the risk assessment, including identified risks, mitigation strategies, and remediation efforts, will be maintained.

3. Data Protection

The following measures are implemented to protect PHI and PII:

- **Data Minimization:** Only collect, process, and store PHI and PII that is necessary f
- **Data Security:** Implement appropriate technical and organizational measures to p
  * Physical Security: Secure storage of paper records in locked cabinets and rooms with controlled access.
  * Electronic Security: Implement strong passwords, anti-malware software, and regular software updates on all devices used to access or process PHI/PII (including workstations, laptops, and mobile devices, if any). Data encryption (at rest and in transit) should be considered for sensitive electronic PHI/PII.
- **Data Retention:** Retain PHI and PII only for as long as necessary to fulfill the purp
- **Data Disposal:** Dispose of PHI and PII securely when it is no longer needed. This in
- **Data Subject Rights (GDPR Compliance):** Establish procedures for responding to d
- **Secure File Sharing:** If electronic file sharing is necessary, use secure methods, su

- **Backup and Recovery:** Implement a regular backup schedule to protect against da

4. Access Controls

Access to PHI and PII will be restricted to authorized personnel based on the principle of least privilege.

- **User Account Management:** Unique user accounts will be created for each individ
- **Password Management:** Users will be required to create strong passwords that m
- **Access Authorization:** Access to PHI and PII will be granted based on job function
- **Termination Procedures:** Access to PHI and PII will be promptly revoked upon ter
- **Physical Access Control:** Restrict physical access to areas where PHI and PII are s

5. Incident Response

An incident response plan will be maintained to address security incidents involving PHI and PII. The plan will include:

- **Incident Identification:** Procedures for identifying and reporting security incidents
- **Incident Containment:** Steps to contain the incident and prevent further damage
- **Incident Eradication:** Measures to remove the cause of the incident (e.g., removi
- **Incident Recovery:** Procedures for restoring systems and data to normal operatio
- **Incident Reporting:** Reporting obligations to relevant authorities (e.g., supervisor
- **Post-Incident Review:** A review of the incident to identify lessons learned and imp

All employees must be trained on the incident response plan and their roles and responsibilities in responding to security incidents.

6. Security Awareness Training

All personnel who access, process, or store PHI and PII will receive security awareness

training on a regular basis (at least annually). The training will cover:

- Data privacy and security principles.
- Common threats and vulnerabilities (e.g., phishing, malware, social engineering).
- Safe computing practices.
- Password management.
- Incident reporting procedures.
- This Cybersecurity Policy and related procedures.
- Data Subject Rights under GDPR and how to respond to requests.

Training will be tailored to the specific roles and responsibilities of personnel. Records of training completion will be maintained.

7. Compliance and Auditing

This policy will be reviewed and updated at least annually to ensure compliance with applicable regulations, including GDPR. Regular audits will be conducted to assess compliance with this policy and identify areas for improvement. These audits may includ

- Review of access controls.
- Review of security awareness training records.
- Review of incident response procedures.
- Review of data retention and disposal practices.
- Internal vulnerability scans of systems that handle electronic PHI/PII (if any).

Audit findings will be documented and reported to management. Corrective actions will implemented to address any identified deficiencies.

8. Conclusion

Protecting the confidentiality, integrity, and availability of PHI and PII is essential to

maintaining the trust of our patients and complying with legal and regulatory requirements. This Cybersecurity Policy provides a framework for achieving these goals. All personnel are responsible for understanding and adhering to this policy. By working together, we can create a secure environment for the protection of sensitive information