1. Introduction

This Cybersecurity Policy outlines the framework for protecting the confidentiality, integrity, and availability of protected health information (PHI) and other sensitive data within our organization. While currently operating in a Low-Risk environment, characterized by limited threat landscape and a strong focus on preventative measures, this policy adheres to the principles of data minimization, purpose limitation, and transparency, as mandated by regulations such as the General Data Protection Regulation (GDPR). This policy applies to all employees, contractors, vendors, and any other individuals or entities accessing or using our organization's systems, networks, and data. The policy's objectives are to mitigate identified risks, ensure compliance with applicable laws and regulations, and foster a security-conscious culture throughout the organization. Regular review and updates will ensure this policy remains effective and aligned with evolving threats and regulatory requirements.

2. Risk Assessment

A comprehensive risk assessment will be conducted at least annually, or more frequently if significant changes occur within the organization's infrastructure, operations, or regulatory landscape. The risk assessment will identify potential threats and vulnerabilities that could compromise the confidentiality, integrity, or availability of PHI and other sensitive data. While our operating environment is currently considered Low-Risk, the assessment will still consider a range of potential threats, including but not limited to:

- Phishing Attacks: Targeting employees to obtain sensitive information or credentials.
- Malware Infections: Introduction of malicious software through email, web browsing, or removable media.
- Unauthorized Access: Gaining access to systems or data without proper authorization.
- Data Breaches: Accidental or intentional disclosure of PHI.
- Physical Security Incidents: Theft or damage to physical assets storing sensitive data.
- Third-Party Risks: Vulnerabilities associated with vendors or partners accessing or processing PHI.

The assessment will evaluate the likelihood and potential impact of each identified risk, and prioritize mitigation efforts accordingly. The results of the risk assessment will inform the development and implementation of appropriate security controls and safeguards.

3. Data Protection

Data protection is paramount. This section outlines the measures for safeguarding PHI and other sensitive data throughout its lifecycle, from creation to disposal.

- Data Minimization: We will collect and retain only the minimum amount of PHI necessary for legitimate business purposes.
- Data Encryption: PHI will be encrypted at rest and in transit using industry-standard encryption algorithms. This includes encrypting data stored on servers, workstations, laptops, and removable media, as well as encrypting data transmitted over networks and the internet.

- Data Masking and Anonymization: When appropriate, data will be masked or anonymized to protect individual identities while still allowing for data analysis and reporting.
- Data Backup and Recovery: Regular backups of critical data will be performed and stored securely in a separate location. Backup and recovery procedures will be tested regularly to ensure data can be restored in the event of a system failure or data loss incident.
- Data Retention and Disposal: Data will be retained only for as long as necessary to fulfill the purposes for which it was collected and in accordance with legal and regulatory requirements. When data is no longer needed, it will be securely disposed of using methods that prevent unauthorized access or disclosure.
- Data Transfers: Transfers of personal data outside of the organization will be subject to careful review to ensure appropriate safeguards are in place, in compliance with GDPR and other relevant regulations. This includes implementing Data Processing Agreements (DPAs) with third-party vendors.

4. Access Controls

Access to PHI and other sensitive data will be strictly controlled based on the principle of least privilege. This means that individuals will only be granted access to the information and resources they need to perform their job duties.

- User Authentication: Strong authentication methods, such as multi-factor authentication (MFA), will be implemented to verify user identities before granting access to systems and data.
- Access Rights Management: User access rights will be reviewed and updated regularly to ensure they remain appropriate. Access will be promptly revoked when an employee leaves the organization or changes roles.
- Role-Based Access Control (RBAC): Access will be granted based on defined roles, ensuring users only have access to the resources required for their specific job functions.
- Password Management: Strong password policies will be enforced, requiring users to create complex passwords and change them regularly. Password reuse will be prohibited.
- Physical Access Controls: Physical access to facilities where PHI is stored will be restricted through measures such as badge access, security cameras, and visitor logs.
- Audit Trails: System activity will be logged and monitored to detect unauthorized access or suspicious behavior. Audit logs will be reviewed regularly.

5. Incident Response

A comprehensive incident response plan will be in place to address security incidents and data breaches in a timely and effective manner.

- Incident Reporting: All employees are required to report any suspected security incidents or data breaches immediately to the designated incident response team.
- Incident Assessment: The incident response team will assess the nature and scope of the incident to determine the appropriate course of action.
- Containment: Immediate steps will be taken to contain the incident and prevent further damage or data loss.
- Eradication: The root cause of the incident will be identified and eliminated.
- Recovery: Systems and data will be restored to their normal operating state.

- Notification: Affected individuals and regulatory authorities will be notified as required by applicable laws and regulations (e.g., GDPR).
- Post-Incident Review: A post-incident review will be conducted to identify lessons learned and improve incident response procedures. The incident response plan will be tested and updated regularly.

6. Security Awareness Training

All employees will receive regular security awareness training to educate them about cybersecurity threats, vulnerabilities, and best practices. Training will cover topics such as:

- Phishing Awareness: Recognizing and avoiding phishing attacks.
- Password Security: Creating and maintaining strong passwords.
- Data Protection: Handling PHI and other sensitive data securely.
- Malware Prevention: Avoiding malware infections.
- Social Engineering: Recognizing and avoiding social engineering attacks.
- Incident Reporting: Reporting suspected security incidents.
- Physical Security: Maintaining physical security of facilities and devices.

Training will be tailored to the specific roles and responsibilities of employees. Ongoing awareness campaigns will be conducted to reinforce key security messages.

7. Compliance and Auditing

This Cybersecurity Policy will be regularly reviewed and updated to ensure compliance with applicable laws and regulations, including GDPR.

- Internal Audits: Internal audits will be conducted periodically to assess the effectiveness of security controls and identify areas for improvement.
- External Audits: External audits may be conducted by independent third parties to provide an objective assessment of the organization's security posture.
- Compliance Monitoring: Ongoing monitoring will be performed to ensure compliance with regulatory requirements.
- Documentation: All security policies, procedures, and documentation will be maintained and updated regularly.
- Data Protection Impact Assessments (DPIAs): DPIAs will be conducted for any new projects or initiatives that involve the processing of personal data, as required by GDPR.

8. Conclusion

This Cybersecurity Policy is essential for protecting our organization's data assets and maintaining the trust of our patients, partners, and stakeholders. By adhering to the principles and guidelines outlined in this policy, we can minimize our risk exposure, ensure compliance with applicable laws and regulations, and foster a security-conscious culture throughout the organization. This policy will be reviewed and updated regularly to ensure it remains effective and aligned with evolving threats and regulatory requirements. All employees are responsible for understanding and complying with this policy.