Cybersecurity Policy for Healthcare Organizations (Low Risk Environment)

--1. Introduction--

This Cybersecurity Policy outlines the essential security practices and controls required to protect the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI) and other sensitive data within this healthcare organization. This policy is designed to meet the requirements of applicable regulations, including but not limited to the Digital Data Risk Ordinance (DDRO), and is tailored for a low-risk environment. All employees, contractors, vendors, and any other individuals accessing or using the organization's information systems and data must adhere to this policy. This policy is a living document and will be reviewed and updated at least annually, or more frequently as required by changes in regulations, technology, or the organization's risk profile.

--2. Risk Assessment--

A comprehensive risk assessment will be conducted at least annually to identify potential threats and vulnerabilities to the organization's information assets. Given the low-risk environment, the assessment will focus on common and easily mitigated risks, such as phishing attacks, weak passwords, and unpatched software. The risk assessment process will involve:

- --Asset Identification:-- Identifying and categorizing all information assets, including hardware, software, data, and systems.
- --Threat Identification:-- Identifying potential threats that could exploit vulnerabilities, such as malware, ransomware, unauthorized access, and data breaches.
- --Vulnerability Assessment:-- Identifying weaknesses in systems, applications, and processes that could be exploited by threats. This will include regular vulnerability scans of all network devices and endpoints using a tool such as Nessus Essentials.
- --Risk Analysis:-- Evaluating the likelihood and impact of identified risks to determine their overall severity.
- --Risk Prioritization:-- Prioritizing risks based on their severity to guide the implementation of appropriate security controls.

The results of the risk assessment will be documented and used to inform the development and implementation of security controls and procedures. A remediation plan with timelines and assigned responsibilities will be created to address identified high-risk vulnerabilities.

--3. Data Protection--

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

- --Data Encryption:-- ePHI and other sensitive data will be encrypted both in transit and at rest using industry-standard encryption algorithms. For data at rest, AES-256 encryption is the minimum acceptable standard. Full disk encryption must be enabled on all laptops and removable media. Data in transit will be protected using TLS 1.2 or higher. Key management will adhere to NIST Special Publication 800-57. Specifically, encryption

keys will be generated, stored, and managed using a secure key management system. Approved systems requiring encryption include but are not limited to: all laptops, servers, databases containing ePHI, and email communication.

- --Data Minimization:-- Only collect, use, and retain the minimum amount of data necessary to achieve the intended purpose. Regularly review data retention policies and securely dispose of data that is no longer needed according to HIPAA guidelines and organizational policy. Data disposal will follow NIST 800-88 guidelines, using methods appropriate for the sensitivity of the data (e.g., secure erase for SSDs, degaussing for magnetic media).
- --Data Backup and Recovery:-- Implement a robust data backup and recovery plan to ensure business continuity in the event of a system failure or data loss. Backups will be performed daily and stored securely, both on-site and off-site. Offsite backups will be geographically diverse to protect against regional disasters. Test the data recovery process quarterly to ensure its effectiveness. Backups will be encrypted using AES-256.
- --Data Loss Prevention (DLP):-- Implement DLP measures to prevent sensitive data from leaving the organization's control. This includes monitoring email traffic for ePHI being sent outside the organization, blocking unauthorized data transfers to USB drives, and educating employees about data handling procedures. DLP rules will be regularly reviewed and updated.
- --Physical Security:-- Protect physical access to data centers, server rooms, and other locations where sensitive data is stored. Implement physical security controls such as badge access controls, surveillance cameras with recording capabilities, and environmental monitoring (temperature and humidity) in server rooms. Access logs will be reviewed monthly.

--4. Access Controls--

Access to ePHI and other sensitive data will be restricted to authorized personnel only. The following access control measures will be implemented:

- --Least Privilege:-- Grant users only the minimum level of access necessary to perform their job duties. Regularly review user access privileges (at least quarterly) and revoke access when it is no longer needed.
- --Strong Passwords:-- Enforce the use of strong passwords that meet minimum complexity requirements (at least 12 characters, including upper and lower case letters, numbers, and symbols) and are changed every 90 days. Implement multi-factor authentication (MFA) for all users accessing sensitive systems and data, including remote access.
- --Account Management:-- Implement a process for creating, modifying, and deleting user accounts. Disable inactive accounts promptly (within 30 days of inactivity).
- --Role-Based Access Control (RBAC):-- Assign access rights based on job roles rather than individual users. This simplifies access management and ensures that users have the appropriate level of access based on their responsibilities. Access roles will be documented and reviewed annually.
- --Audit Trails:-- Maintain audit trails of all access to ePHI and other sensitive data. Regularly review audit logs (at least monthly) to detect and investigate unauthorized access attempts. Implement an automated log monitoring system (SIEM light) to alert on suspicious activity.

--5. Incident Response--

A documented incident response plan will be maintained to address security incidents and data breaches promptly and effectively. The plan will include:

- --Incident Identification:-- Procedures for identifying and reporting security incidents. Employees are required to report any suspected security incidents to the IT department or designated security personnel immediately.
- --Containment:-- Steps to contain the impact of a security incident and prevent further damage. This includes isolating affected systems from the network, disabling compromised accounts, and implementing emergency firewall rules.
- --Eradication:-- Procedures for removing the cause of the security incident. This includes removing malware, patching vulnerabilities, and reconfiguring systems.
- --Recovery:-- Steps to restore affected systems and data to their normal state. This includes restoring from backups, rebuilding systems, and verifying data integrity.
- --Post-Incident Analysis:-- A review of the incident to identify lessons learned and improve security controls. A formal post-incident report will be created documenting the incident, response actions, and recommendations for improvement.
- --Reporting:-- Procedures for reporting security incidents to relevant authorities, as required by law and regulation (e.g., HIPAA breach notification). The incident response plan will define reporting timelines and responsible parties. The legal and compliance departments will be consulted for all breach notifications.

The incident response plan will be tested at least annually through tabletop exercises or simulated attacks to ensure its effectiveness. Key roles and responsibilities within the incident response team include:

- --Incident Commander:-- Overall responsibility for managing the incident response.
- --Technical Lead:-- Responsible for technical analysis and containment efforts.
- --Communications Lead:-- Responsible for internal and external communications.
- --Legal Counsel:-- Responsible for legal and regulatory compliance.

--6. Security Awareness Training--

All employees, contractors, and vendors will receive regular security awareness training (at least annually) to educate them about cybersecurity risks and best practices. The training will cover topics such as:

- --Phishing Awareness:-- Recognizing and avoiding phishing attacks. Simulated phishing exercises will be conducted periodically to assess employee awareness.
- --Password Security:-- Creating and maintaining strong passwords.
- --Data Handling:-- Protecting sensitive data from unauthorized access and disclosure.
- --Social Engineering:-- Recognizing and avoiding social engineering attacks.
- --Mobile Security:-- Protecting mobile devices and data.
- --Incident Reporting:-- Procedures for reporting security incidents.
- --Acceptable Use Policy:-- Understanding and adhering to the organization's acceptable use policy for IT resources.

Training will be tailored to the specific roles and responsibilities of different user

groups. Documentation of completed training will be maintained.

--7. Technical Controls--

The following technical controls will be implemented to enhance security:

- --Firewall:-- A firewall will be deployed at the network perimeter to control network traffic. Firewall rules will be reviewed and updated regularly. Default rules will be to deny all traffic unless specifically allowed.
- --Intrusion Detection System (IDS):-- A network-based IDS will be implemented to monitor network traffic for malicious activity. Alerts will be reviewed and investigated promptly.
- --Security Information and Event Management (SIEM):-- A basic SIEM solution will be implemented to collect and analyze security logs from various systems. The SIEM will be configured to generate alerts for suspicious activity. The solution will utilize a cloud offering like AWS CloudWatch or Azure Sentinel.
- --Endpoint Detection and Response (EDR):-- EDR software will be deployed on all endpoints (desktops, laptops, servers) to detect and respond to threats. EDR will include features such as behavioral analysis, threat intelligence integration, and automated response capabilities.
- --Vulnerability Management:-- A regular vulnerability scanning program will be implemented to identify and remediate vulnerabilities in systems and applications. Scans will be conducted monthly, and critical vulnerabilities will be patched within 72 hours.
- --Antivirus/Antimalware:-- Antivirus/antimalware software will be deployed on all endpoints and kept up-to-date with the latest definitions.

--8. Compliance and Auditing--

This policy will be reviewed and updated at least annually to ensure compliance with applicable laws, regulations, and industry best practices, including DDRO. Regular audits will be conducted to verify compliance with this policy and identify areas for improvement. These audits will include:

- --Policy Review:-- Reviewing the policy to ensure it is up-to-date and aligned with current regulations and best practices.
- --Technical Assessments:-- Conducting vulnerability scans and penetration tests to identify weaknesses in systems and applications. Penetration tests will be conducted annually by a qualified third party.
- --Compliance Audits:-- Assessing compliance with specific regulations, such as DDRO. The policy fulfills DDRO Article 5 by implementing appropriate technical and organizational measures to protect personal data. -Specifically, Section 3 (Data Protection) addresses DDRO Article 5(a) by implementing data encryption, anonymization, and pseudonymization techniques. Section 4 (Access Controls) addresses DDRO Article 5(b) by restricting access to personal data to authorized personnel only. Section 7 (Technical Controls) addresses DDRO Article 5(c) by ensuring the security of processing systems and services. Section 5 (Incident Response) addresses DDRO Article 5(d) by establishing procedures for responding to security incidents involving personal data. Section 8 (Compliance and Auditing) ensures ongoing compliance as required by the DDRO.-
- --Third-Party Audits:-- Engaging independent third-party auditors to assess the

organization's security posture.

Audit findings will be documented and used to develop corrective action plans.

--9. Digital Data Risk Ordinance (DDRO) Compliance Mapping--

This section provides a specific mapping of policy sections to DDRO articles. This is not exhaustive but highlights key areas of compliance.

--DDRO Article--	--Policy Section(s)--	--Description--
--Article 5: Data Security--	3 (Data Protection), 4 (Access Control), 7 (Technical Controls), 8 (Incident Re	Implement technical and organizational m
--Article 6: Data Minimization--	3 (Data Minimization)	Ensures that only the minimum necessary per
--Article 7: Purpose Limitation--	3 (Data Minimization)	Data is only collected and used for specified,
--Article 9: Breach Notification--	5 (Incident Response)	Establishes procedures for reporting data brea
--Article 10: Data Retention--	3 (Data Minimization)	Defines data retention periods and procedure

--10. Conclusion--

This Cybersecurity Policy is essential for protecting ePHI and other sensitive data within this healthcare organization. By implementing the security controls and procedures outlined in this policy, the organization can mitigate cybersecurity risks and maintain compliance with applicable regulations. All personnel are responsible for adhering to this policy and contributing to a secure environment. Continued vigilance, training, and adherence to this policy will help ensure the ongoing protection of sensitive information and the trust of our patients and stakeholders.