Cybersecurity Policy for Healthcare Organizations (Low Risk Environment)

1. Introduction

This Cybersecurity Policy outlines the minimum-security standards and practices that [Organization Name] employs to protect the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI) and other sensitive data. This policy is designed to comply with applicable regulations, including the California Consumer Privacy Act (CCPA), and reflect a risk-based approach appropriate for a low-risk environment. All employees, contractors, vendors, and other individuals or entities accessing or using [Organization Name]'s information systems are required to adhere to this policy. Non-compliance may result in disciplinary action, up to and including termination of employment or contract.

2. Risk Assessment

[Organization Name] conducts periodic risk assessments, at least annually, to identify potential threats and vulnerabilities to its information systems and data. These assessments will consider:

- Asset Identification: Identifying and categorizing all assets that store, process, or transmit ePHI and other sensitive data.
- Threat Identification: Identifying potential threats to these assets, including but not limited to malware, phishing, unauthorized access, and data breaches.
- Vulnerability Assessment: Assessing the vulnerabilities present in our systems and processes that could be exploited by identified threats.
- Likelihood and Impact Analysis: Evaluating the likelihood of a threat exploiting a vulnerability and the potential impact on the organization and its patients.
- Risk Prioritization: Prioritizing risks based on their potential impact and likelihood of occurrence.

The results of the risk assessment will be used to inform the development and implementation of security controls. In a low-risk environment, the focus will be on implementing cost-effective controls that address the most critical risks.

3. Data Protection

[Organization Name] is committed to protecting the privacy and security of ePHI and other sensitive data. The following data protection measures will be implemented:

- Data Minimization: Collecting and retaining only the minimum amount of data necessary for legitimate business purposes.
- Data Encryption: Encrypting ePHI at rest and in transit, whenever feasible, using industry-standard encryption algorithms. This includes encrypting laptops and other portable devices that may contain ePHI.
- Data Masking/De-identification: Employing data masking or de-identification techniques to protect sensitive data when it is not needed in its complete form, particularly for research or analytics purposes.
- Data Backup and Recovery: Regularly backing up ePHI and other sensitive data to a secure offsite location. Testing the restoration process periodically to ensure data can be

recovered in the event of a disaster or system failure.

- Data Disposal: Securely disposing of ePHI and other sensitive data when it is no longer needed, in accordance with applicable regulations. This includes shredding paper documents and securely wiping electronic media.
- CCPA Compliance: Ensuring compliance with the California Consumer Privacy Act (CCPA) by providing consumers with the right to know what personal information is collected, the right to delete personal information, and the right to opt-out of the sale of personal information. [Organization Name] does not sell personal information. We will maintain a clear and accessible privacy policy outlining these rights. We will also establish procedures for responding to consumer requests under the CCPA.

4. Access Controls

[Organization Name] implements access controls to ensure that only authorized individuals can access ePHI and other sensitive data. These controls include:

- User Authentication: Requiring strong passwords and multi-factor authentication (MFA) where feasible for accessing systems that contain ePHI.
- Role-Based Access Control (RBAC): Granting users access to only the data and resources they need to perform their job duties. Access rights will be reviewed and updated regularly.
- Least Privilege: Granting users the minimum necessary access rights to perform their job functions.
- Account Management: Establishing procedures for creating, modifying, and terminating user accounts promptly. Dormant accounts will be disabled.
- Physical Security: Restricting physical access to facilities and systems that store, process, or transmit ePHI. This includes using access badges, security cameras, and other security measures.
- Remote Access: Securing remote access to the network through the use of VPNs and MFA.

5. Incident Response

[Organization Name] has established an incident response plan to effectively address security incidents that may compromise the confidentiality, integrity, or availability of ePHI or other sensitive data. The incident response plan will include:

- Incident Detection: Implementing mechanisms to detect security incidents, such as intrusion detection systems and security information and event management (SIEM) systems.
- Incident Reporting: Establishing procedures for employees to report suspected security incidents. All employees are responsible for reporting any suspected security breaches immediately to [Designated Contact/Department].
- Incident Containment: Taking immediate steps to contain security incidents to prevent further damage.
- Incident Eradication: Removing the cause of the security incident.
- Incident Recovery: Restoring affected systems and data to normal operation.
- Post-Incident Activity: Analyzing the incident to identify lessons learned and improve security controls.
- Breach Notification: Complying with all applicable breach notification requirements under

state and federal law, including notification to affected individuals and regulatory agencies.

6. Security Awareness Training

[Organization Name] provides regular security awareness training to all employees, contractors, and vendors who access or use its information systems. The training will cover topics such as:

- Data security policies and procedures
- Phishing awareness
- Password security
- Social engineering awareness
- Malware prevention
- Physical security
- Reporting security incidents
- Compliance with CCPA and other applicable regulations

Training will be conducted at least annually and upon onboarding new personnel.

7. Compliance and Auditing

[Organization Name] will conduct periodic audits to ensure compliance with this Cybersecurity Policy and applicable regulations, including the CCPA.

- Policy Review: This policy will be reviewed and updated at least annually, or more frequently as needed, to reflect changes in the threat landscape, regulations, or business operations.
- Vulnerability Scanning: Regular vulnerability scanning will be performed to identify and remediate vulnerabilities in our systems.
- Penetration Testing: Periodic penetration testing may be conducted to assess the effectiveness of security controls.
- Audit Logging: Audit logs will be maintained to track user activity and system events. These logs will be reviewed regularly to detect suspicious activity.
- Third-Party Risk Management: Performing due diligence on third-party vendors who access or process ePHI to ensure they have adequate security controls in place.

8. Conclusion

This Cybersecurity Policy demonstrates [Organization Name]'s commitment to protecting the privacy and security of ePHI and other sensitive data. By adhering to this policy, all employees, contractors, and vendors contribute to maintaining a secure environment and protecting the trust of our patients. This policy is a living document and will be updated periodically to reflect changes in the threat landscape and regulatory environment.