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. 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. This includes hardware, software, data, and physical locations.
- Threat Identification: Identifying potential threats to these assets, including but not limited to malware, phishing, unauthorized access, data breaches, and insider threats.
- Vulnerability Assessment: Assessing the vulnerabilities present in our systems and processes that could be exploited by identified threats. This includes regular vulnerability scanning and penetration testing.
- Likelihood and Impact Analysis: Evaluating the likelihood of a threat exploiting a vulnerability and the potential impact on the organization and its patients. Impact will be assessed based on potential financial loss, reputational damage, legal repercussions, and disruption of services.
- Risk Prioritization: Prioritizing risks based on their potential impact and likelihood of occurrence. Risks will be categorized as high, medium, or low, and mitigation plans will be developed accordingly.

The results of the risk assessment will be used to inform the development and implementation of security controls.

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 retention periods will be defined and enforced.
- Data Encryption: Encrypting ePHI at rest and in transit, whenever feasible, using industry-standard encryption algorithms (e.g., AES-256). This includes encrypting laptops and other portable devices that may contain ePHI. Encryption keys will be securely managed.
- 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. De-identification methods will comply with HIPAA standards.

- Data Backup and Recovery: Regularly backing up ePHI and other sensitive data to a secure offsite location. Backups will be performed daily, and full backups will be performed weekly. Testing the restoration process periodically (at least quarterly) to ensure data can be recovered in the event of a disaster or system failure. Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) will be defined and tested.
- 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 using methods that meet or exceed NIST standards.
- 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, as well as procedures for submitting requests. We will also establish procedures for responding to consumer requests under the CCPA within the legally mandated timeframe, including processes for verifying the identity of the requestor.

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. Password complexity requirements include a minimum length of 12 characters, a mix of upper and lowercase letters, numbers, and symbols. Account lockout policies will be implemented after a specified number of failed login attempts (e.g., 5 attempts). Session timeout settings will be configured to automatically log users out after a period of inactivity (e.g., 15 minutes).
- 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, at least quarterly, and upon changes in job responsibilities.
- 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 after 60 days of inactivity and deleted after 90 days.
- 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. Media handling procedures will be implemented to ensure that physical media (e.g., hard drives, tapes) are securely stored and disposed of. Workstation security measures will include locking workstations when unattended and prohibiting the installation of unauthorized software.
- Remote Access: Securing remote access to the network through the use of VPNs and MFA. Remote access will be granted only to authorized individuals and will be subject to

regular review.

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, security information and event management (SIEM) systems, and regular review of audit logs.
- 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] via [Designated Reporting Method].
- Incident Containment: Taking immediate steps to contain security incidents to prevent further damage. This may include isolating affected systems, disabling compromised accounts, and implementing temporary security measures.
- Incident Eradication: Removing the cause of the security incident. This may include removing malware, patching vulnerabilities, and reconfiguring systems.
- Incident Recovery: Restoring affected systems and data to normal operation. This may include restoring from backups, rebuilding systems, and verifying data integrity.
- Post-Incident Activity: Analyzing the incident to identify lessons learned and improve security controls. A post-incident report will be created documenting the incident, the response, and the lessons learned.
- Breach Notification: Complying with all applicable breach notification requirements under state and federal law, including notification to affected individuals and regulatory agencies within required timeframes.

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
- Proper use of company resources
- Data privacy best practices

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

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. Scans will be performed at least quarterly, and high-risk vulnerabilities will be remediated within 30 days.
- Penetration Testing: Periodic penetration testing may be conducted to assess the effectiveness of security controls. Penetration tests will be performed at least annually by a qualified third party.
- Audit Logging: Audit logs will be maintained to track user activity and system events. These logs will be reviewed regularly (at least monthly) to detect suspicious activity. Log retention policies will be established and enforced.
- 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. This includes conducting vendor security assessments, reviewing vendor security policies, and including security requirements in contracts. Vendor assessments will be conducted annually or more frequently if significant changes occur.
- Vendor Security Assessments: Prior to engaging a third-party vendor that will have access to ePHI or other sensitive data, a security assessment will be conducted. This assessment will evaluate the vendor's security policies, procedures, and controls.
- Contractual Requirements: Contracts with third-party vendors will include clauses requiring them to comply with applicable security regulations and to protect the confidentiality, integrity, and availability of ePHI. These clauses will also address data breach notification requirements and liability.

8. Policy Enforcement

The [Designated Department/Role] is responsible for enforcing this Cybersecurity Policy. Violations of this policy may result in disciplinary action, up to and including termination of employment or contract. The [Designated Department/Role] will also monitor compliance with this policy and report any violations to management. The policy will be communicated to all employees, contractors and vendors.