Cybersecurity Policy for Healthcare (Low Risk Environment)

--1. Introduction--

This Cybersecurity Policy outlines the framework for protecting the confidentiality, integrity, and availability of electronic protected health information (ePHI) and other sensitive data within our healthcare organization. This policy is designed to be compliant with the California Consumer Privacy Act (CCPA) and is tailored for a low-risk environment, acknowledging our current operational scale and the sensitivity of the data we manage. All employees, contractors, vendors, and other individuals accessing our systems and data must adhere to this policy. Its purpose is to establish clear guidelines and expectations for maintaining a secure environment, protecting patient privacy, and ensuring business continuity.

--2. Risk Assessment--

We conduct regular risk assessments to identify, analyze, and prioritize potential threats and vulnerabilities to our information assets. These assessments consider the likelihood and impact of potential security incidents, taking into account factors such as data sensitivity, system criticality, and threat landscape. Due to the low-risk classification, our focus is on implementing foundational security controls and mitigating common threats such as phishing, malware, and unauthorized access. Risk assessments are reviewed and updated at least annually, or more frequently if significant changes occur in our environment or threat landscape.

--3. Data Protection--

- --Data Minimization:-- We collect and retain only the minimum amount of personal information necessary for legitimate business purposes, in accordance with CCPA principles.
- --Data Encryption:-- Sensitive data, including ePHI, is encrypted both in transit and at rest. Encryption standards used must be compliant with industry best practices.
- --Data Loss Prevention (DLP):-- Measures are in place to prevent sensitive data from leaving the organization's control. This includes monitoring data transfer activities and implementing controls to block unauthorized data exfiltration.
- --Data Backup and Recovery:-- Regular backups of critical data are performed and stored securely. Recovery procedures are tested periodically to ensure data can be restored in a timely manner in the event of a data loss incident.
- --Data Disposal:-- Data is securely disposed of when it is no longer needed for business purposes, using methods that prevent unauthorized access or recovery. Physical media is shredded and electronic data is securely wiped.

--4. Access Controls--

- --Principle of Least Privilege:-- Access to systems and data is granted only to those individuals who require it to perform their job duties.
- --User Authentication:-- Strong passwords are required for all user accounts. Multi-factor authentication (MFA) is encouraged, especially for access to sensitive systems and data.
- --Access Reviews:-- User access rights are reviewed regularly to ensure they remain

appropriate and necessary. Terminated employees' access is revoked immediately.

- --Account Management:-- Procedures are in place for creating, modifying, and disabling user accounts. A central directory service is used to manage user identities and access rights.
- --Physical Security:-- Physical access to our facilities and data centers is restricted to authorized personnel. Security measures such as access badges, surveillance cameras, and alarm systems are in place.

--5. Incident Response--

- --Incident Response Plan:-- A documented incident response plan outlines the procedures for detecting, analyzing, containing, eradicating, and recovering from security incidents.
- --Incident Reporting:-- All employees are responsible for reporting suspected security incidents immediately to the designated incident response team.
- --Incident Analysis:-- Security incidents are thoroughly analyzed to determine the root cause and identify any necessary corrective actions.
- --Containment and Eradication:-- Measures are taken to contain the impact of security incidents and prevent further damage. Infected systems are isolated and malware is removed.
- --Recovery:-- Systems and data are restored to normal operation as quickly as possible after a security incident.
- --Post-Incident Review:-- A post-incident review is conducted to evaluate the effectiveness of the incident response plan and identify areas for improvement.
- --Breach Notification:-- In the event of a data breach involving personal information, we will comply with all applicable notification requirements under CCPA and other relevant regulations.

--6. Security Awareness Training--

- --Annual Training:-- All employees receive annual security awareness training that covers topics such as phishing awareness, password security, data protection, and incident reporting.
- --Phishing Simulations:-- Periodic phishing simulations are conducted to test employee awareness and identify areas for improvement.
- --Policy Updates:-- Employees are notified of any updates or changes to this Cybersecurity Policy.
- --Ongoing Education:-- Regular security awareness tips and reminders are provided to employees to reinforce key security concepts.

--7. Compliance and Auditing--

- --CCPA Compliance:-- This policy is designed to be compliant with the California Consumer Privacy Act (CCPA). We adhere to the principles of data minimization, transparency, and user rights under the CCPA.
- --Regular Audits:-- Internal audits are conducted periodically to assess compliance with this Cybersecurity Policy and identify any gaps or weaknesses.
- --Policy Review:-- This Cybersecurity Policy is reviewed and updated at least annually, or more frequently if necessary to reflect changes in our environment, threat landscape, or

regulatory requirements.

- --Documentation:-- All security policies, procedures, and controls are documented and maintained.
- --Reporting:-- We provide regular reports to management on the status of our cybersecurity program and any identified risks or vulnerabilities.

--8. Conclusion--

This Cybersecurity Policy is essential for protecting the confidentiality, integrity, and availability of our data and systems. By adhering to this policy, we can minimize the risk of security incidents, protect patient privacy, and ensure compliance with applicable regulations. All employees are expected to understand and follow this policy, and to actively participate in maintaining a secure environment. Continuous improvement and adaptation are necessary to stay ahead of evolving threats and ensure the ongoing effectiveness of our cybersecurity program.