# Cybersecurity Policy for Healthcare Organizations

### 1. Introduction

This Cybersecurity Policy outlines the security standards and procedures that [Organization Name] will adhere to in order to protect the confidentiality, integrity, and availability of its information assets. This policy applies to all employees, contractors, vendors, and other authorized users who access or use [Organization Name]'s systems and data. As a healthcare organization operating in a medium-risk environment, we acknowledge the sensitive nature of Protected Health Information (PHI) and other confidential data we handle, and this policy is designed to mitigate associated risks while adhering to relevant compliance standards, specifically SOC 2, HIPAA, and other applicable regulations. The effectiveness of this policy relies on the participation and diligence of every member of our organization.

### 2. Risk Assessment

[Organization Name] will conduct regular risk assessments to identify, analyze, and prioritize cybersecurity risks. These assessments will cover all aspects of our information systems, including infrastructure, applications, and data.

- --Frequency:-- Risk assessments will be conducted at least annually, and more frequently when significant changes occur in our environment (e.g., new systems, regulations, or threats), or following a significant security incident.
- --Methodology:-- Assessments will employ a recognized risk management framework (e.g., NIST Cybersecurity Framework, ISO 27005, HITRUST CSF) and will consider both internal and external threats, vulnerabilities, and potential impacts.  This includes both qualitative and quantitative analysis where appropriate.
- --Scope:-- The scope of risk assessments will include but not be limited to:
- Data security and privacy risks associated with PHI and other sensitive information.
- Risks related to third-party vendors and business associates.
- Technological vulnerabilities in systems and applications.
- Operational risks related to processes and procedures.
- Compliance with relevant regulations (e.g., HIPAA, SOC 2).
- --Remediation:-- Identified risks will be documented, prioritized, and addressed according to their potential impact and likelihood. Remediation plans will be developed and implemented, with progress tracked and reported to senior management via a risk register. Remediation efforts will be documented, including exceptions and compensating controls where applicable.

### 3. Vulnerability Management

[Organization Name] will maintain a robust vulnerability management program to identify, assess, and remediate security vulnerabilities in our systems and applications.

- --Vulnerability Scanning:-- Regular vulnerability scans will be conducted on all systems and applications using industry-standard scanning tools.  Scans will be performed at least quarterly, and more frequently for critical systems.  Authenticated and unauthenticated scans will be utilized where appropriate.

- --Patch Management:-- A formal patch management process will be implemented to ensure that security patches are applied promptly and effectively. Patches will be tested in a non-production environment before being deployed to production systems. A risk-based approach will be used to prioritize patching, with critical vulnerabilities addressed within [defined timeframe, e.g., 72 hours] and high vulnerabilities addressed within [defined timeframe, e.g., 30 days]. Exception requests must be formally documented and approved.
- --Vulnerability Assessment:-- Identified vulnerabilities will be assessed to determine their potential impact and likelihood of exploitation. Assessments will consider factors such as CVSS scores, exploit availability, and the sensitivity of the affected data. Penetration testing will be conducted annually by a qualified third party to validate the effectiveness of security controls and identify exploitable vulnerabilities.
- --Remediation Tracking:-- All identified vulnerabilities will be tracked and remediated in a timely manner. Remediation efforts will be documented, and progress will be reported to senior management. A vulnerability register will be maintained to track the status of all identified vulnerabilities.

### 4. Data Protection

[Organization Name] is committed to protecting the confidentiality, integrity, and availability of all data, especially PHI.

- --Data Classification:-- Data will be classified based on its sensitivity and criticality. This classification will dictate the appropriate security controls for storage, access, and transmission. Data classification levels will include, but are not limited to: Public, Internal, Confidential, and Restricted.
- --Data Encryption:-- Sensitive data, both in transit and at rest, will be encrypted using industry-standard encryption algorithms. Encryption keys will be securely managed using a key management system. Acceptable encryption algorithms include:
- --Data at Rest:-- AES-256 (Advanced Encryption Standard) or higher.
- --Data in Transit:-- TLS 1.2 or higher. Strong ciphersuites must be configured.

Encryption keys will be stored separately from the encrypted data.

- --Data Loss Prevention (DLP):-- DLP measures will be implemented to prevent the unauthorized disclosure or loss of sensitive data. This includes monitoring data movement, controlling access to sensitive files, and educating users on data handling best practices. DLP solutions will be configured to monitor for sensitive data patterns and prevent data exfiltration through email, web browsing, and removable media.
- --Data Backup and Recovery:-- Regular backups of critical data will be performed and stored in a secure, offsite location. Data recovery procedures will be documented and tested at least annually to ensure business continuity and disaster recovery. Backup retention policies will be defined based on regulatory requirements and business needs. RTO (Recovery Time Objective) and RPO (Recovery Point Objective) will be defined for critical systems.
- --Data Retention and Disposal:-- Data will be retained only as long as necessary for business or legal requirements, adhering to HIPAA guidelines for PHI. Data will be securely disposed of using methods that prevent unauthorized access or recovery, such as data wiping or physical destruction. A data retention schedule will be maintained.

### 5. Access Controls

Access to systems and data will be restricted based on the principle of least privilege.

- --User Account Management:-- User accounts will be created, managed, and terminated according to a defined process. Strong passwords and multi-factor authentication (MFA) will be required for all user accounts accessing sensitive systems and data. Password complexity requirements will include: [Specify requirements, e.g., Minimum 12 characters, upper and lower case letters, numbers, and symbols]. Passwords will be rotated every [defined timeframe, e.g., 90 days].
- --Role-Based Access Control (RBAC):-- Access permissions will be granted based on job roles and responsibilities. Access rights will be reviewed and updated at least annually, and upon any changes to job responsibilities.
- --Privileged Access Management (PAM):-- Access to privileged accounts will be strictly controlled and monitored using a PAM solution. Privileged access will be granted only when necessary and will be subject to enhanced security measures, such as just-in-time access and session recording.
- --Remote Access:-- Remote access to [Organization Name]'s network will be secured using VPNs and MFA. Remote access policies will be enforced to ensure secure connections and data transmission. Approved VPN protocols include: [Specify approved protocols, e.g., IPSec, OpenVPN].
- --Physical Security:-- Physical access to data centers, server rooms, and other sensitive areas will be restricted and monitored using access control systems, surveillance cameras, and security personnel. Access logs will be reviewed regularly.

### 6. Incident Response

[Organization Name] will maintain a comprehensive incident response plan to detect, analyze, contain, eradicate, and recover from cybersecurity incidents.

- --Incident Detection:-- Systems and networks will be monitored for suspicious activity using Security Information and Event Management (SIEM) systems and intrusion detection/prevention systems (IDS/IPS). Alerts will be triaged by a security operations center (SOC) or designated security personnel.
- --Incident Reporting:-- All suspected security incidents must be reported immediately to the designated incident response team via [defined reporting method, e.g., helpdesk, email, phone].
- --Incident Response Team:-- A dedicated incident response team will be responsible for investigating and responding to security incidents. The team will include representatives from IT, security, legal, and communications.
- --Incident Response Procedures:-- The incident response plan will outline detailed procedures for handling different types of security incidents, including data breaches, malware infections, ransomware attacks, and system outages. The plan will be tested at least annually through tabletop exercises and simulated incidents.
- --Post-Incident Review:-- Following a security incident, a post-incident review will be conducted to identify the root cause of the incident, evaluate the effectiveness of the incident response plan, and implement corrective actions to prevent future incidents.
- --Notification Procedures:-- The incident response plan will include procedures for

notifying affected parties, including patients, regulators (e.g., HHS for HIPAA breaches), and law enforcement, as required by law and regulations. Notification timelines will adhere to regulatory requirements.

### 7. Change Management

[Organization Name] will implement a formal change management process to ensure that all changes to our IT environment are properly planned, tested, and implemented in a secure manner.

- --Change Request Process:-- All changes to systems, applications, and infrastructure must be submitted through a formal change request process. The change request must include a detailed description of the proposed change, the reason for the change, the potential impact of the change, and a backout plan.
- --Change Approval:-- Change requests must be reviewed and approved by a change management board (CAB), which will include representatives from IT, security, and other relevant departments. The CAB will assess the risks associated with the change and ensure that it is aligned with the organization's security policies and procedures.
- --Testing and Validation:-- All changes must be thoroughly tested in a non-production environment before being deployed to production. Testing should include functional testing, security testing, and performance testing.
- --Implementation and Monitoring:-- Changes will be implemented according to a defined schedule and will be monitored closely to ensure that they are implemented correctly and that they do not have any unintended consequences.
- --Documentation:-- All changes will be documented in a change log, including the date of the change, the person who made the change, and the reason for the change.

### 8. Third-Party Risk Management

[Organization Name] will implement a comprehensive third-party risk management program to assess and mitigate the risks associated with using third-party vendors and business associates.

- --Vendor Due Diligence:-- Before engaging with a third-party vendor, a thorough due diligence process will be conducted to assess their security posture. This includes reviewing their security policies, procedures, and certifications (e.g., SOC 2, ISO 27001), and conducting security questionnaires and risk assessments. A minimum security standard will be established for all vendors handling sensitive data.
- --Contractual Requirements:-- Contracts with third-party vendors will include specific security requirements, such as data protection clauses, incident response obligations, and audit rights. Business Associate Agreements (BAAs) will be in place with all vendors who handle PHI, as required by HIPAA.
- --Ongoing Monitoring:-- The security posture of third-party vendors will be monitored on an ongoing basis through regular reviews of their security performance, vulnerability scans, and penetration tests. Vendors will be required to provide evidence of their compliance with security requirements.
- --Vendor Risk Rating:-- Each vendor will be assigned a risk rating based on the sensitivity of the data they handle, their access to our systems, and their overall

security posture. Vendors with higher risk ratings will be subject to more frequent and rigorous monitoring.
- --Termination Procedures:-- Contracts with third-party vendors will include procedures for terminating the relationship in the event of a security breach or other violation of the security requirements. Procedures for secure data return or destruction will be defined.

### 9. Security Awareness Training

All employees, contractors, and vendors will receive regular security awareness training to educate them about cybersecurity threats and best practices.

- --Training Content:-- Training will cover topics such as:
- Phishing awareness.
- Password security.
- Data handling procedures.
- Social engineering.
- Incident reporting.
- Acceptable use of company resources.
- HIPAA compliance (for those handling PHI).
- Secure coding practices (for developers).
- --Training Frequency:-- Security awareness training will be conducted at least annually, and more frequently for high-risk individuals (e.g., those with privileged access) and new hires.
- --Training Delivery:-- Training will be delivered through a variety of methods, including online modules, in-person presentations, simulated phishing exercises, and security newsletters.
- --Training Tracking:-- Completion of security awareness training will be tracked and reported to management. Training records will be maintained for audit purposes.

### 10. Compliance and Auditing

[Organization Name] is committed to complying with all applicable laws, regulations, and industry standards, including SOC 2, HIPAA, and other relevant regulations.

- --SOC 2 Compliance:-- This policy is designed to support [Organization Name]'s SOC 2 compliance efforts. We will implement and maintain controls to meet the SOC 2 Trust Services Criteria (e.g., Security, Availability, Processing Integrity, Confidentiality, Privacy).
- --HIPAA Compliance:-- We will comply with all applicable HIPAA regulations, including the Privacy Rule, the Security Rule, and the Breach Notification Rule.
- --Internal Audits:-- Regular internal audits will be conducted at least annually to assess the effectiveness of security controls and compliance with this policy. Audit findings will be documented and tracked to resolution.
- --External Audits:-- External audits will be performed by qualified third-party auditors to verify compliance with SOC 2, HIPAA, and other applicable regulations. Audit reports will be reviewed by senior management.
- --Policy Review:-- This policy will be reviewed and updated at least annually, or more frequently as needed to address changes in the threat landscape, regulations, or business

operations.  The policy review date will be documented.

- --Documentation:-- All security policies, procedures, and controls will be documented and maintained in a central repository.  Documentation will be reviewed and updated regularly.

### 11. Conclusion

This Cybersecurity Policy is essential for protecting [Organization Name]'s information assets and ensuring the privacy and security of patient data. By adhering to this policy, we can mitigate cybersecurity risks, maintain compliance with applicable regulations, and build trust with our patients, partners, and stakeholders. Every member of our organization is responsible for understanding and following this policy. Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract. This policy is approved by [Name and Title] and is effective as of [Date].