**Information Security Policy: ABC Medical Company**

Steven Sturgeon

SEC 4303-18.02.01-5B25-S1: IS Security Policy Analysis

Professor Krahenbill

5/27/2025

# **Information Security Policy**

### **1.1 Purpose**

The purpose of this Information Security Policy is to establish a comprehensive framework to protect the confidentiality, integrity, and availability of all information assets managed by ABC Medical Company. Given the sensitive nature of healthcare information and our legal obligations under the Health Insurance Portability and Accountability Act (HIPAA), this policy ensures that appropriate administrative, technical, and physical safeguards are in place to mitigate risks and prevent unauthorized access, use, or disclosure of protected health information (PHI).

This policy also aligns with recognized standards such as NIST SP 800-53 and ISO/IEC 27001 to promote best practices in healthcare cybersecurity and risk management.

### **1.2 Scope**

This policy applies to:

* All employees, contractors, interns, and third-party service providers who access ABC Medical Company’s information systems or data.
* All information systems, applications, networks, hardware, and electronic media that store, transmit, or process sensitive or regulated data, including PHI and personally identifiable information (PII).
* All physical and digital environments under the control of ABC Medical Company, including remote work and mobile device use.

This policy covers organizational and technical controls as they pertain to data governance, access control, security operations, compliance, and incident response.

### **1.3 Risk Statement**

ABC Medical Company operates in a highly regulated environment where the confidentiality, integrity, and availability of sensitive health information are paramount. Failure to secure protected health information (PHI) and personally identifiable information (PII) can result in serious consequences, including regulatory penalties under HIPAA, reputational damage, loss of patient trust, and operational disruption due to cybersecurity incidents.

This policy is designed to mitigate the following key risks:

* **Unauthorized access** to sensitive systems and data (PHI leaks or insider threats)
* **Malware infections and phishing attacks** targeting employees and endpoints
* **Data loss or corruption** due to insufficient backup or secure development practices
* **Compliance violations** from gaps in training, policy enforcement, or documentation
* **Physical breaches** resulting in stolen or damaged devices and media
* **Unsecured remote access** to critical systems during telework or vendor support

## **2. Acceptable Use**

### **2.1 Email Use**

Email is a critical communication tool at ABC Medical Company, but it also poses risks of unauthorized data disclosure and phishing. To protect sensitive information:

* Company email accounts must be used for all work-related communications; personal accounts are prohibited.
* Transmission of PHI via email is only permitted when the email is encrypted or sent through a secure messaging platform.
* All emails are scanned for malware, phishing, and spam using advanced email security gateways.
* Employees must report suspicious emails immediately to the IT or security team.
* Auto-forwarding of company emails to external accounts is not allowed.
* Training on email security awareness, including phishing simulations, is provided at least annually.

### **2.2 Internet and Web Access**

ABC Medical Company provides internet access to support business operations, and all users are expected to use it responsibly. The following rules apply:

* Internet access is monitored and filtered to block malicious or inappropriate websites.
* Accessing websites known to host malware, illegal content, or peer-to-peer file sharing is strictly prohibited.
* Streaming media or excessive bandwidth usage for non-business purposes is not permitted.
* Downloading software or browser plugins must be pre-approved by the IT department.
* Users must not attempt to bypass internet filters or security controls.

## **3. System and Data Protection**

### **3.1 Application Development Security**

ABC Medical Company ensures that all internally developed or externally procured applications undergo secure software development practices. This includes:

* Conducting security risk assessments during the development lifecycle.
* Following OWASP guidelines to prevent common vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure authentication.
* Implementing input validation, error handling, and session management safeguards.
* Conducting code reviews and vulnerability scanning before deployment.
* Requiring multi-factor authentication (MFA) and encrypted communications (e.g., TLS 1.2 or higher) in all web-based applications that transmit PHI or PII.

### **3.2 Data Backup and Storage**

To ensure data availability and integrity, ABC Medical Company enforces regular data backup and secure storage practices:

* Backups of critical systems and PHI are performed daily and stored in an encrypted format.
* Backup media are stored offsite or in a secure cloud environment that meets HIPAA requirements.
* Backup restoration procedures are tested quarterly to validate data integrity and recovery speed.
* Physical and cloud storage must enforce access controls and encryption at rest.

### **3.3 Data Handling**

All handling of sensitive information (including PHI and PII) must follow strict access control and classification rules:

* Data must be classified (public, internal, confidential, regulated) and labeled accordingly.
* PHI must only be accessed, used, or disclosed by authorized personnel on a need-to-know basis.
* Encryption (AES-256 or equivalent) is required for all portable devices and transmissions involving sensitive data.
* Disposal of media containing PHI must follow NIST 800-88 guidelines, ensuring complete data destruction.

## **4. Network and Device Security**

### **4.1 Network Device Installation and Configuration**

All network devices such as but not limited to routers, switches, firewalls at ABC Medical Company must be installed and configured securely to prevent unauthorized access or data leakage. Key controls include:

* Only authorized IT personnel may configure network infrastructure.
* Default credentials must be changed, and unused services disabled before deployment.
* All devices must be configured to log security events and forward them to a centralized logging solution.
* Firewall rules and access control lists (ACLs) must be reviewed quarterly to ensure least-privilege access.
* Network segmentation is enforced to isolate sensitive systems, including electronic health record (EHR) platforms, from general-purpose networks.

### **4.2 Device Security**

All computing devices such as but not limited to desktops, laptops, mobile devices used to access ABC Medical Company systems must comply with the following standards:

* Full disk encryption (FDE) is mandatory for all portable devices.
* Devices must have endpoint protection software with real-time malware scanning.
* Idle session timeouts, password protection, and automatic screen locks must be configured.
* All devices must receive security patches and updates regularly via automated tools or documented procedures.
* Personal devices (BYOD) are prohibited from accessing systems containing PHI unless enrolled in the company’s mobile device management (MDM) platform.

### **4.3 Remote Access**

Remote access to ABC Medical Company’s network is restricted and secured using the following measures:

* All remote access must occur over a virtual private network (VPN) with strong encryption (IPsec or SSL VPN with MFA).
* Access is granted based on role and requires managerial and IT approval.
* PHI must not be stored locally on remote devices unless explicitly approved and encrypted.
* Remote sessions are logged and monitored for suspicious activity.

## **5. Physical and Environmental Security**

### **5.1 Facility Access Controls**

* Access to offices, data centers, and server rooms is restricted to authorized personnel only and enforced via electronic keycard and/or biometric access systems.
* All visitors must be logged, escorted, and issued temporary badges that expire after use.
* Physical security logs (entry/exit records) are retained for at least 6 months for auditing purposes.
* Facilities are equipped with surveillance systems (CCTV) in sensitive areas, monitored regularly by security personnel or designated staff.

### **5.2 Workstation Security**

* Workstations located in public or shared spaces must have privacy screens and be positioned to prevent shoulder surfing or unauthorized viewing.
* Employees must lock their workstations when unattended and log off at the end of the workday.
* Unauthorized personnel may not use company workstations or access devices containing PHI.

### **5.3 Equipment and Media Protection**

* Servers and network equipment are stored in secure, climate-controlled rooms with fire suppression systems.
* Electronic media and portable storage devices must be encrypted and logged for accountability.
* Disposal of equipment or storage media must follow NIST SP 800-88 guidelines to ensure complete data sanitization.
* Lost or stolen devices must be reported immediately to the IT department for investigation and incident response.

## **6. Policy Awareness and Communication**

### **6.1 Stakeholder Identification**

Stakeholders include:

* Executive leadership
* All employees and contractors
* IT and security teams
* Compliance and legal personnel
* Third-party service providers with access to ABC systems or data

### **6.2 Distribution and Accessibility**

* The Information Security Policy is stored in a centralized internal portal accessible to all employees.
* Any updates or revisions are communicated promptly via company-wide announcements, emails, or team briefings.
* The latest version of the policy must be reviewed and acknowledged by all new hires during onboarding.

### **6.3 Awareness and Training**

* All employees must complete security awareness training annually, which includes a review of key policies, HIPAA requirements, phishing simulations, and incident reporting procedures.
* Specialized training is provided for technical staff, developers, and anyone handling PHI.
* Completion of training is tracked and reported to management for accountability.

### **6.4 Feedback and Enforcement**

* Employees are encouraged to ask questions and provide feedback on security policies through HR or designated compliance contacts.
* Failure to comply with the policy may result in disciplinary actions, up to and including termination, depending on the severity of the violation.
* Policy compliance is subject to periodic audits and is part of the organization’s continuous risk management program.

## **7. Policy Administration**

### **7.1 Non-Compliance**

All employees, contractors, and third parties are expected to comply with this Information Security Policy. Violations may result in disciplinary action, including loss of access privileges, formal reprimand, suspension, termination, and legal action where applicable. Violations involving PHI will be reported in accordance with HIPAA breach notification requirements.

### **7.2 Policy Review and Updates**

This policy is reviewed annually, or as needed in response to:

* Changes in applicable laws and regulations (HIPAA, state privacy laws),
* Updates to organizational structure or systems,
* Results from audits or risk assessments.

The Chief Information Security Officer (CISO) and Compliance Officer are responsible for maintaining and approving this policy.

### **7.3 Related Documents/References**

* Center for Internet Security. (2021). *CIS critical security controls for effective cyber defense version 8.* <https://www.cisecurity.org/controls/v8>
* International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO/IEC Standard No. 27001:2022). <https://www.iso.org/standard/27001>
* National Institute of Standards and Technology. (2014). *Guidelines for media sanitization* (NIST Special Publication 800-88 Revision 1). <https://doi.org/10.6028/NIST.SP.800-88r1>
* National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53 Rev. 5). <https://doi.org/10.6028/NIST.SP.800-53r5>
* National Institute of Standards and Technology. (2024). *Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A cybersecurity resource guide* (NIST Special Publication 800-66 Revision 2). <https://doi.org/10.6028/NIST.SP.800-66r2>
* Open Worldwide Application Security Project. (2021). *OWASP Top ten web application security risks.* <https://owasp.org/Top10/>
* SANS Institute. (2025). *Information security policy templates.* <https://www.sans.org/information-security-policy/>
* U.S. Department of Health & Human Services. (2023). *Health Insurance Portability and Accountability Act of 1996 (HIPAA).* <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>

### **7.4 Document Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Description** | **Author** |
| 1.0 | 2025-05-07 | Initial release | IT Security Department |

## **Appendix A: Control Mapping Matrix**

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy Section** | **Framework** | **Control ID(s)** | **Control Description** |
| 2.1 Email Use | NIST SP 800-53 Rev. 5 | SC-12, SI-3, SI-4 | Encryption, malware protection, system monitoring |
| 2.1 Email Use | ISO/IEC 27002:2022 | 5.10, 8.24 | Acceptable use, email use policies |
| 2.1 Email Use | HIPAA Security Rule | §164.312(e)(1) | Transmission security (email encryption) |
| 2.2 Internet & Web Access | NIST SP 800-53 Rev. 5 | SC-7, SC-18, AC-17 | Boundary protection, content filtering, remote access |
| 2.2 Internet & Web Access | ISO/IEC 27002:2022 | 5.10, 8.1, 8.23 | Acceptable use, user access, web filtering |
| 2.2 Internet & Web Access | HIPAA Security Rule | §164.312(b) | Audit controls for internet usage |
| 3.1 Application Development Security | NIST SP 800-53 Rev. 5 | SA-11, SI-10, CM-2 | Secure development lifecycle, flaw remediation, configuration mgmt |
| 3.1 Application Development Security | ISO/IEC 27002:2022 | 8.25, 8.9 | Secure application development, access control |
| 3.1 Application Development Security | HIPAA Security Rule | §164.308(a)(1)(ii)(A) | Risk analysis for custom applications |
| 3.2 Data Backup and Storage | NIST SP 800-53 Rev. 5 | CP-9, CP-10 | Backup and recovery planning and testing |
| 3.2 Data Backup and Storage | ISO/IEC 27002:2022 | 5.28, 8.13 | Information backup, storage protection |
| 3.2 Data Backup and Storage | HIPAA Security Rule | §164.308(a)(7) | Contingency planning (data backup) |
| 3.3 Data Handling | NIST SP 800-53 Rev. 5 | MP-5, SC-12, SC-28 | Media sanitization, encryption, protection of data at rest |
| 3.3 Data Handling | ISO/IEC 27002:2022 | 5.12, 8.10 | Data classification, secure disposal |
| 3.3 Data Handling | HIPAA Security Rule | §164.310(d)(2) | Media reuse and disposal procedures |
| 4.1 Network Device Installation | NIST SP 800-53 Rev. 5 | AC-4, SC-7, AU-6 | Access control, boundary protection, audit review |
| 4.1 Network Device Installation | ISO/IEC 27002:2022 | 8.20, 8.21 | Network security management, firewall configuration |
| 4.2 Device Security | NIST SP 800-53 Rev. 5 | CM-7, SI-3, AC-19 | Configuration control, malware defense, mobile device access |
| 4.2 Device Security | ISO/IEC 27002:2022 | 5.11, 8.1 | Device protection and access control |
| 4.2 Device Security | HIPAA Security Rule | §164.310(c) | Workstation security |
| 4.3 Remote Access | NIST SP 800-53 Rev. 5 | AC-17, SC-12 | Remote access control, encryption |
| 4.3 Remote Access | ISO/IEC 27002:2022 | 5.15, 8.26 | Remote access policies, secure communications |
| 4.3 Remote Access | HIPAA Security Rule | §164.312(a)(1) | Access control for remote users |
| 5.1 Facility Access Controls | NIST SP 800-53 Rev. 5 | PE-2, PE-3, PE-6 | Physical entry controls, monitoring, visitor access |
| 5.1 Facility Access Controls | ISO/IEC 27002:2022 | 7.4, 7.5 | Physical entry and monitoring controls |
| 5.1 Facility Access Controls | HIPAA Security Rule | §164.310(a)(1) | Facility access control measures |
| 5.2 Workstation Security | NIST SP 800-53 Rev. 5 | PE-20, AC-11 | Workstation protection, session locks |
| 5.2 Workstation Security | ISO/IEC 27002:2022 | 8.5 | Workstation use procedures |
| 5.2 Workstation Security | HIPAA Security Rule | §164.310(c) | Workstation security implementation |
| 5.3 Equipment and Media Protection | NIST SP 800-53 Rev. 5 | MP-5, MP-6 | Media transport and sanitization |
| 5.3 Equipment and Media Protection | ISO/IEC 27002:2022 | 8.10, 8.11 | Equipment maintenance and secure disposal |
| 5.3 Equipment and Media Protection | HIPAA Security Rule | §164.310(d)(2) | Media reuse and disposal procedures |
| 6.1–6.4 Policy Awareness and Communication | NIST SP 800-53 Rev. 5 | AT-2, PL-4, PM-13 | Security awareness training, policy updates |
| 6.1–6.4 Policy Awareness and Communication | ISO/IEC 27002:2022 | 6.3, 6.4 | Information security awareness and communication |
| 6.1–6.4 Policy Awareness and Communication | HIPAA Security Rule | §164.308(a)(5) | Security awareness and training procedures |

## **Appendix B: Definitions and Glossary**

**PHI (Protected Health Information)** — Individually identifiable health information that is transmitted or maintained in any form or medium, subject to HIPAA regulations.

**PII (Personally Identifiable Information)** — Information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, or biometric records.

**Encryption** — The process of converting information into a secure format that is unreadable without a decryption key.

**MFA (Multi-Factor Authentication)** — A security mechanism that requires two or more verification factors to gain access to a system or resource.

**Endpoint Protection** — Security solutions that protect end-user devices such as desktops, laptops, and mobile devices from cyber threats.

**Access Control** — The selective restriction of access to data or systems based on user roles and permissions.

**Audit Trail** — A record showing who accessed a system and what operations they performed during a given period.

**Secure Development Lifecycle (SDLC)** — A process that integrates security practices within the software development lifecycle.

**Media Sanitization** — The process of rendering access to target data on media infeasible for a given level of effort.

**Risk Assessment** — The process of identifying, estimating, and prioritizing risks to organizational operations and assets.

**Incident Response** — A structured approach to managing and responding to a cybersecurity incident.

**VPN (Virtual Private Network)** — A secure tunnel that encrypts data as it travels over public networks to private systems.

## **Appendix C: Roles and Responsibilities Matrix**

|  |  |  |
| --- | --- | --- |
| **Role** | **Responsibility** | **Relevant Policy Areas** |
| Chief Information Security Officer (CISO) | Oversees the development, implementation, and maintenance of the organization’s information security program. Ensures policies are aligned with applicable standards and regulations. | All sections; Policy Review and Updates |
| IT Security Team | Implements and manages security technologies, monitors network traffic, enforces access control, and responds to incidents. | Network and Device Security, System and Data Protection, Remote Access |
| Compliance Officer | Ensures organizational adherence to legal and regulatory requirements including HIPAA. Supports audits and maintains documentation. | Data Handling, Policy Administration |
| Department Managers | Ensure team members follow security policies and complete required training. Report non-compliance or incidents. | Policy Awareness and Communication, Acceptable Use |
| All Employees and Contractors | Comply with security policies, report suspicious activity, complete required security training. | Acceptable Use, Physical Security, Policy Awareness |
| HR and Training Coordinators | Coordinate policy training and ensure employees acknowledge policies during onboarding. | Policy Awareness and Communication |
| Third-Party Vendors | Comply with ABC Medical Company’s security requirements when accessing company data or systems. | Remote Access, Data Handling |

## **Appendix D: HIPAA Security Rule Crosswalk**

|  |  |  |  |
| --- | --- | --- | --- |
| **HIPAA Safeguard** | **HIPAA Citation** | **Policy Section(s)** | **Control Description / Application** |
| Administrative Safeguards | §164.308(a)(1) | 1.1 Purpose, 6.3 Awareness and Training | Risk management and workforce security training |
| Administrative Safeguards | §164.308(a)(5) | 6.3 Awareness and Training | Security awareness and training programs |
| Administrative Safeguards | §164.308(a)(7) | 3.2 Data Backup and Storage | Contingency planning and data backup |
| Administrative Safeguards | §164.308(a)(1)(ii)(D) | 6.4 Feedback and Enforcement | Sanction policy for non-compliance |
| Physical Safeguards | §164.310(a)(1) | 5.1 Facility Access Controls | Control and validation of physical access to facilities |
| Physical Safeguards | §164.310(c) | 4.2 Device Security, 5.2 Workstation Security | Workstation use and physical safeguards |
| Physical Safeguards | §164.310(d)(2) | 3.3 Data Handling, 5.3 Equipment and Media Protection | Media reuse and disposal procedures |
| Technical Safeguards | §164.312(a)(1) | 4.3 Remote Access | Access control for systems handling PHI |
| Technical Safeguards | §164.312(b) | 2.2 Internet and Web Access | Audit controls for network and web activity |
| Technical Safeguards | §164.312(e)(1) | 2.1 Email Use | Transmission security via encryption for PHI |