

Information security policy template for healthcare organizations

Why do you need an information security policy?

Healthcare organizations are routinely managing the sensitive health information of their patients. Cybercrimes are steadily on the rise and healthcare has always been one of the most targeted industries by cybercriminals.

It is vital for employees to be made aware of the risks of not following the security guidelines set by industry regulations like HIPAA. This customizable template can be a guide for healthcare organizations to set forth the expectations and requirements the employees must meet to ensure the security of all PII and ePHI handled within the organization.

Table of Contents

Introduction.....	3
Scope.....	3
Policy.....	3
Employee Responsibilities and Requirements.....	3
Security Awareness Training.....	4
Access Control.....	4
Password Policy.....	5
Network Management.....	5
Handling of Sensitive Information.....	6
Remote Work.....	7
Operations Security.....	8
Data Security Protection.....	9
Transportable Media.....	9
Disposal of Media.....	10
Change Management.....	10
Information Security Incidents.....	10
Audit Controls.....	11
Maintaining Information Security and Business Continuity.....	11
Breach of Policy.....	12
Acknowledgment Form.....	13

_____: Information Security Policy

1. Introduction

The information security policy of _____ defines the rules and responsibilities employees, contractors and other temporary employees must follow to ensure the safety and integrity of data generated and processed by _____ as well the personal health information and personally identifiable information of patients.

2. Scope

This policy is applicable to all employees, contractors, and temporary employees working within the premises of _____ and other remote locations approved by _____.

3. Policy

3.1. Employee Responsibilities and Requirements

- All employees must have an ID card. All visitors with the exception of patients must wear a visitor's badge.
- All unattended computers and other mobile devices should be locked when leaving the work area.
- An automatic screen lock function will be deployed to the devices with the help of a Mobile Device Management solution.
- Employees will be prohibited from taking any actions to override this setting. Only computer hardware and software owned by and installed by _____ is permitted to be connected to or installed on _____ equipment.
- Personal devices supplied by the _____ are to be used only for business purposes.
- No configuration changes and modifications will be allowed on these devices. All software programs and documentation provided by or generated by the employees, consultants or contractors for the benefit of _____ are the property of the _____ unless stated otherwise in a contractual agreement.
- This won't be applicable to software purchased by employees at their own expense.

3.2. Security Awareness Training

- The _____ shall take up the responsibility to conduct the initial security training.
- In addition to the general security policies and procedures of _____, employees shall also be briefed on the requirements of the HIPAA Security Rule and any updates to the HIPAA regulations found within the Health Information Technology for Economic and Clinical Health (HITECH) Act.
- Security training shall be given to new employees during the orientation process. Participation in such trainings shall be mandatory for all employees.
- Documentation of all training activities must be maintained.

3.3. Access Control

3.3.1. User Logon IDs

- Individual users shall have unique logon IDs and passwords.
- An access control system shall identify each user and prevent unauthorized users from entering or using information resources.
- Security requirements for user identification will include the assignment of a unique identifier and the responsibility of users for the use and misuse of their individual logon ID.
- All user login IDs are audited at least _____ and all inactive logon IDs are to be revoked. _____ Human Resources Department shall notify the _____ of the departure of the employee and contractor, at which time the login IDs will be revoked.
- Information resources are protected by the use of strict access control systems. It includes both internal (passwords, encryption, access control lists) and external (port protection devices, firewalls, host-based authentication) controls.
- Authentication based on a “need to know” basis is a requirement of the HIPAA regulation. Users will be added to the information system and network only upon the approval of their supervisors/department heads.

3.3.2. Review of User Logins

- If an employee changes position at the _____, the employee’s new supervisor or department head shall promptly notify the _____ of the change of roles and the access that needs to be added in order to provide the employee access to data to effectively perform their new job responsibilities.

- The _____ must conduct entitlement reviews with department heads on an annual basis to ensure that all employees have the appropriate roles, access and software necessary to perform their jobs properly while being limited to the minimum necessary data to facilitate HIPAA compliance and protection of patient data.

3.3.3. Termination of User Logon Account

- Upon termination of an employee, the employee's supervisor or department head should immediately notify the _____.
- The employee's department head shall be responsible to ensure that all keys, ID cards, other access devices as well as _____ equipment and property is returned to the _____ on the final day of their employment.
- The _____ and the _____ shall provide a list of active user accounts for network and application access, including access to the clinical electronic health record (EHR) to the department heads for review.
- Department heads shall review the employee access lists within _____ business days of receipt. If any of the employees on the list are no longer employed by _____, the department head will immediately notify the _____ of the employee's termination status.

3.4. Password Policy

- User IDs and passwords are required in order to gain access to all _____ networks and workstations.
- The passwords will be restricted by a corporate wide password policy, which will be pushed to the devices via a Mobile Device Management solution.

3.5. Network Management

3.5.1. Internet Access

- Internet access is provided for _____ users and should not be used for unproductive purposes.
- The company wide usage of these non-business sites consumes a large amount of internet bandwidth, which can render the internet unserviceable for responsible users and lead to downtime.
- Individual internet usage will be monitored by the means of a Mobile Device Management solution.

- If an employee is found to be consuming huge amounts of bandwidth for personal use, disciplinary action will be taken. Employees must follow these rules regarding Internet usage:
 - Prior approval from the _____ should be obtained before accessing the internet or any other external network connection.
 - Users are not permitted to install or download any software. If users have a need for additional software, they must follow the _____ change management process and contact the supervisor.
 - The network can be used to market services related to the _____. Use of the network for personal profit is prohibited.
 - Confidential data including credit card numbers, login passwords and other parameters should be encrypted before being transmitted through the Internet.
 - The encryption software used, and the specific encryption keys shall be escrowed with the _____ to ensure they are safely maintained or stored.
 - The use of encryption software and keys, which have not been escrowed shall be prohibited and may subject the user to disciplinary action.

3.5.2. Electronic Communication and Email

- All electronic communication messages generated or handled by _____ owned equipment is considered the property of the _____.
- No PHI or PII should be send via e-mail unless it is encrypted. All sensitive data and files shall be encrypted before its transmission through networks.
- Resources provided by the _____ intended only for business purposes.

3.6. Handling of Sensitive Information

- Confidentiality of the information should be maintained in accordance with the policies imposed by the _____.
- All employees must recognize the sensitive nature of data maintained by _____ and hold all data in the strictest confidence.
- Any purposeful release of data to which an employee may have access is a violation of _____ policy and will result in immediate termination and legal action.

3.6.1. Confidentiality Agreement

- In order to gain access to _____ resources, employees must sign a confidentiality agreement.
- Temporary workers and third-party employees are required to sign the agreement prior to being given access to _____ information resources.
- The agreements will be reviewed when there are any changes to the contracts or other terms of employment.

3.6.2. Transferring Data

- When transferring data to the _____ remotely, it should be done only via an approved VPN connection to ensure the integrity and confidentiality of the data being transferred.

3.7. Remote Work

- Remote work shall only be accepted with prior permission from the concerned supervisor.
- The rules defined below is applicable to all employees working permanently or temporarily outside of _____ premises:
 - Employees will have access to information only on a 'need to know' basis.
 - Strong password policies will be pushed to the devices and remote employees are expected to be compliant with them.
 - Work cannot resume unless the employee has all the applications and software installed on the devices. These will be pushed via a Mobile Device Management solution.
 - The devices should run on the following operating systems

3.7.1. Securely transferring files and other data remotely

- Employees are prohibited from installing or using any personal software within the _____ devices.
- If a need for specific software exists, the employee must follow the change management policy and submit a request to their concerned supervisor.
- Users shall not use _____ purchased software on home computers or other equipment not approved by _____.

- Confidential data of _____ including but not limited to patient information, IT Systems information, financial information or human resource data, shall not be placed on any property not owned by _____ without obtaining the written consent of the respective supervisor.
- The _____ Wide Area Network (WAN) is maintained with a wide range of security protections in place, such as e-mail file type restrictions, firewalls, etc.
- Work containers shall be created on personal devices via a Mobile Device Management solution, where the security measures mentioned above will be maintained.

3.8. Operations Security

3.8.1. Software distribution

- Only software approved by the _____ will be used on internal computers and networks.
- All new software shall be tested to ensure compatibility with the installed software and network configuration.

3.8.2. Lock screen

- Screen time out will be automatically enabled on the devices after _____ of inactivity.

3.8.3. Remote deployment

- Updates and patches will be pushed out via a Mobile Device Management solution to individual workstations and servers on a periodic basis.

3.8.4. External System Access

- Prior permission from supervisors or department heads should be obtained before accessing systems outside the purview of _____.

3.8.5. Clear desk policy

- Employees are expected to follow the clear desk policy set by _____.
- All paper records should be locked in a file cabinet when employees leave their designated work areas. The same applies to remote employees as well.

3.8.6. Retention of Ownership

- All documents and software programs created or provided by employees or contractors for work purposes will be the property of _____ unless stated otherwise by a contractual agreement.
- Employees developing programs or documentation should sign an agreement acknowledging _____ ownership at the time of employment. This will not be applicable to software purchased by employees at their own expense.

3.8.7. Disposal of Equipment

- An inventory should be maintained for all equipment, including older computers. Once the equipment has served its purpose it must be securely disposed.

3.9. Data Security Protection

3.9.1. Data Backup

- Backup procedures have been established to encrypt all sensitive and critical data.
- Recovery tests of the backups shall be done to ensure business continuity of _____ in the event of the occurrence of any natural or man-made disasters.

3.9.2. Data Protection

- Employees are obligated to protect all data within their possession.
- They must ensure to store data only in encrypted spaces and see to it that the old data is deleted as soon as their purpose is complete.

3.10. Transportable Media

- Transportable media will include but are not limited to, SD cards, DVDs, CD-ROMs, USB tokens, flash drives, etc.
- Employees will only be permitted to use transportable media by carefully abiding by the rules listed below:
 - Sensitive data cannot be stored on transportable media unless it is encrypted.
 - Only _____ approved transportable media shall be permitted.
 - Users should not connect the transportable media to a workstation that is not approved by _____.

3.11. Disposal of Media

- All paper containing sensitive information, when no longer needed should be securely disposed of by the means of a shredder.
- Employees working from home or other remote locations must have access to a shredder.
- All external media should be destroyed in accordance with the HIPAA compliance procedures.

3.12. Change Management

- All changes made to the systems should be properly logged. Necessary backups should be maintained prior to the implementation of any changes.
- The change management process should be documented and made available to all employees.
- No changes can be implemented without the approval of the _____.
- The employee implementing the change should be familiar with the rollback process in the event if the change causes any adverse effect within the systems.

3.13. Information Security Incidents

3.13.1. Reporting Software Malfunctions

- Users should inform the appropriate _____ personnel when the user's software does not appear to be functioning correctly. This could pose an information security risk.

3.13.2. Report Security Incidents

- It is the responsibility of each employee or contractor to report security incidents on a continuous basis to the appropriate supervisor.
- Users are to formally report all security incidents or violations of the security policy immediately to the _____.
- Reports of security incidents shall be escalated as quickly as possible. Each member of the _____ must inform the other members as soon as possible.
- Each incident will be analyzed to determine if changes to the existing security structure are necessary. All reported incidents will be logged and appropriate remedial actions will be taken.
- Security breaches shall be promptly investigated. If criminal action is suspected, the _____ shall contact the appropriate law enforcement authorities immediately.

3.14. Audit Controls

- Information systems that contain ePHI must be examined at periodic intervals with the help of technical and managerial audit controls.
- These controls are critical in keeping a record of computer activities. An audit trail can help determine the cause of a security violation and provide security measures to rectify those occurrences.
- _____ shall do a risk evaluation on an ongoing basis and keep track of potential vulnerabilities to the ePHI in possession.
- An adequate amount of technical and security controls shall be implemented in accordance with the HIPAA Security Rule.

3.15. Maintaining Information Security and Business Continuity

3.15.1. Data Backup Plan

- A data backup plan shall be implemented to maintain copies of the ePHI. Incremental backups shall be done _____.
- Monthly backup shall be maintained at all times in a remote location.
- The _____ shall monitor the storage and removal of backups and ensure that all the controls are properly enforced.
- A recovery test shall be conducted _____ to ensure exact copies of ePHI can be effectively retrieved and made available.

3.15.2. Disaster Recovery Plan

- The _____ shall take up the responsibility to develop and update the disaster recovery plan.
- The purpose of the plan being the restoration and recovery of ePHI and to make ePHI available at times of emergency.
- An inventory should be maintained of all hardcopy forms and documents related to clinical, registration and financial interactions with patients.
- Contact information of the _____ should be made available to all employees.
- The _____ on an annual basis should test the effectiveness of the disaster recovery plan and submit its the reports to the _____.

3.16. Breach of Policy

- In the event if an employee violates the _____ privacy and security policies and/or violates the HIPAA or related state laws governing the protection of sensitive patient identifiable information, appropriate disciplinary actions shall be carried out based on the severity of the breach.
- Employees who commit a breach of less severity will get a verbal or written reprimand from their concerned supervisor.
- Data breaches of extreme severity will result in immediate termination and legal action.

_____: Acknowledgement Form

Employee Information

Name: _____

Job Title: _____

Department: _____

Name of Supervisor: _____

I have read, fully understand and accept all the requirements and expectations put forward within the policy.

Employee: _____

Supervisor: _____