Information Security: a Checklist for Healthcare Professionals (2000)

This practice brief has been updated. See the latest version here. This version is made available for historical purposes only.

There are many aspects to consider in protecting the confidentiality of both paper-based and computer-based health information. Healthcare organizations should develop policies and procedures to address these issues with input from a multidisciplinary group that understands the organization's risks and security needs. The Health Insurance Portability and Accountability Act of 1996 has brought information security to the forefront for healthcare organizations.

The following list, while not exhaustive, outlines basic tenets in information security for healthcare professionals to follow in designing, using, and maintaining their health information systems.

Screening Processes

- Pre-employment screening processes are used for employment candidates who will have access to patient records or health information.

Employee Awareness

- Security training is provided to all levels of staff.
- Employees are instructed on how to report breaches.
- Employees, students, and volunteers receive specific training about the confidentiality of health information and their responsibilities.
- Employees, students, and volunteers sign a confidentiality agreement at the time of employment and a statement acknowledging their ongoing responsibility at least once a year thereafter.
- Employees, students, and volunteers understand their responsibilities for respecting patients' privacy and protecting the confidentiality of their health information.
- Computer systems are set up to warn employees if they try to access confidential information.

Physician Awareness

- The organization's medical staff bylaws or rules and regulations outline physician responsibilities for protecting the confidentiality of health information.
- Physicians sign a confidentiality statement at the time of appointment or reappointment to the medical staff.

Patient Awareness

- Patients are educated about their right to confidentiality of health information.

- Patients or their legal representative(s) have access to health information (unless state law prohibits such access).
- There is a clearly defined process for patients or their legal representative(s) to amend incorrect or incomplete health information in their records.

Access Control

- The organization has written policies outlining who may access patient information. Policies and procedures should address access authorization, establishment, and modification. Different types of access are:
    - Mandatory—Fixed security attributes are designated to users and files that limit access.
    - Discretionary—Typically used to restrict access to a file. The owner of the file controls access of users.
    - Time-of-day—Access is restricted by specified times, such as 8 a.m. to 5 p.m.
    - Classification—Multiple levels of access are required depending on the sensitivity of the data.
    - Subject-object separation—Access to subject does not mean automatic access to related objects.
- There are mechanisms in place to control access to both paper and computer-based patient records. These mechanisms apply to all settings where records are kept in the organization, including physician offices that may have access to the organization's information system.
- There is a written organizational policy prohibiting the disclosure or sharing of passwords, access codes, key cards, or other user identifiers. The policy is strictly enforced.
- Passwords contain at least seven alphanumeric characters to make them more difficult to decode.
- Passwords are changed frequently and users are limited to one log-on at a time.
- Use of a secondary level of authentication, such as a password linked to one of the following: biometric identification, an additional password, personal identification, telephone callback, or token.
- Each user's access is restricted to the information needed to do his or her job.
- If a user attempts to access information beyond his or her security clearance with repeated use of an improper code, the system locks the user out or sounds an alarm.
- When a user leaves the facility, his or her password and access codes are deactivated immediately.
- The organization performs routine audits to monitor system activity, including access, log-ins, updates, and edits.
- Access to computer-based records is tracked by individual user to discourage unauthorized viewing.
- The information system limits mass copying, printing, or downloading of patient records.
- Periodic audits are done to see if the organization's policies are current and in line with accreditation standards and state and federal laws.
- If inactive paper-based or computer-based records are archived, they are protected from loss, defacement, or unauthorized disclosure.
- Access controls are in place for clinical systems such as laboratory, radiology, and nuclear medicine.
- Appropriate measures are in place to protect the organization's computer system from unauthorized remote access risks. (Dial-up access enables outsiders to make repeated attempts to gain access without being visible to the

organization using the system.)

- Policies and procedures addressing physical access control are established to limit physical access to an organization. Areas that should be covered in these policies are:
    - Equipment control into and out of the organization
    - Sign-in and escorts for visitors, if appropriate
    - Need-to-know procedures
    - An organization security plan
    - Maintenance records
    - Locks
    - Key distribution

- Policies and procedures are in place for workstation use, such as logging off a computer terminal prior to leaving the work area or automatic logoff after a predetermined time period of inactivity on a system or at a terminal.

Sensitive Data

- Appropriate mechanisms are in place to protect sensitive patient and employee health information. This may include information relating to HIV test results, lifestyle, substance abuse, psychological profiles, or behavioral health records.

- If there is an employee assistance program, employee information is protected from unauthorized disclosure. Employees participating in the program know who will have access to their counseling records.

- When printed reports containing confidential information are no longer needed (such as extra copies of transcribed reports), they are disposed in a manner that protects their confidentiality (shredding, pulping, or burning).

- If paper-based records are recycled when they are no longer needed, they are shredded, pulped, or otherwise handled in a way that will protect the confidentiality of the information they contain. Simply bundling records and sending them to a recycling center does not protect them.

Sabotage

- The organization has a strictly enforced policy that prohibits employees from loading unauthorized software onto the organization's computers.

- Anti-virus software is used to help detect and block computer viruses and other forms of sabotage.

Theft

- Steps have been taken to secure laptop and desktop computers from theft.

- Information on laptop and desktop computers is password protected, so it cannot be easily accessed if the equipment is stolen.

Financial Data

- There are adequate measures to protect patient-related financial data that contain diagnostic or procedural codes and other information that may reveal the reason for treatment.

Electronically Transmitted Data

- If patient health information is transmitted electronically (such as tape-to-tape billing for third-party payers), the recipient has signed a confidentiality agreement, and mechanisms are in place to ensure information is transmitted to the proper individual or entity.

- Encryption is used when information is transmitted over the Internet.

- User authentication or identification is used in conjunction with encryption to prevent unauthorized access.

- E-mail that contains sensitive and confidential information is protected from unauthorized access, alteration and disclosure.

Contractor or Vendor Agreements

- If the organization uses contractors or vendors to provide services that involve health information (statistical processing, photocopying, transcription, storage/retrieval, microfilming, scanning, destruction of information, or information systems support), the contractors or vendors have signed confidentiality agreements and have confidentiality statements on file for their employees or agents.

- The organization has a chain-of-trust agreement with all third parties with access to patient health information. The agreements state that the third party will:

    - Keep the information in strict confidence.
    - Use the information only for the purpose of providing services under the contract.
    - Disclose the information only to those of the third party's employees who need access to the information in order to provide services under the work contract and who have signed an agreement requiring the employee to hold the information in confidence.
    - Return the information in usable form upon request or at the end of the work contract.
    - Indemnify the organization for all breaches of these obligations.

- The work contract contains a warranty that the vendor will not insert any virus, key locks, or other programs into the system, whether or not a dispute exists between the two parties.

Disaster Recovery

- Information systems are backed up periodically and the backup data is maintained off site in a secure location. The frequency of the backup procedure is determined by the organization's needs.

- There is a contingency plan in place for immediate implementation in the event of a disaster, and key employees understand the plan and their roles. The contingency plan includes the following:

    - Applications and data criticality analysis
    - Data backup plan
    - Disaster recovery plan
    - Emergency mode operation plan
    - Testing and revisions as needed

- The organization carries business interruption insurance.

- There is a recovery "hot site" available for continuing business as usual.

- Critical components of the information system are included in the organization's uninterrupted power supply.

- Fire prevention equipment has been installed in the data center and key data storage areas.

Information Services

- Systems managers, network managers, and programmers do not have unlimited and unrecorded access to patient information. All access privileges are assigned on a need-to-know basis, and access of all users is tracked.
- Testing of new systems with live data is limited as much as possible. If test data identify individual patients, test reports and temporary files are destroyed or deleted as soon as possible.
- Help desk personnel cannot view a copy of a user's screen without the user's knowledge. Help desk personnel have been adequately trained to understand their responsibility for maintaining the confidentiality of patient information.
- If workstations are connected to the Internet, firewalls, gateways, or other mechanisms are in place to protect against unauthorized access.
- If confidential information is transmitted via the Internet, it is encrypted to protect it during transmission.

Health Information Management

- The facility identifies an information security officer to oversee information security efforts, policies, and procedures.
- If an outside transcription vendor has modem access to the organization's dictation system, that access is limited appropriately.
- If an outside vendor has access to the organization's computer system (such as a transcription vendor), the vendor can access only the information needed to perform the required service, and that access is limited to read-only. For example, an outside transcription vendor should have access only to the patient's name, hospital number, date of admission, date of discharge, and attending physician.
- If dictated information is transported on cassette tapes or other media, procedures are in place to protect it from loss or unauthorized access. Dictation is erased when no longer needed.
- If an outside vendor (such as a transcription vendor) keeps copies of an organization's reports, the written contract outlines the length of time the copies are to be kept, the form in which they will be kept, who has access to them, and limits the vendor's use of the information.
- If employees transcribe, code, or handle other patient information from home offices, procedures are in place to protect the confidentiality of that information.

Patient Accounts

- The confidentiality of billing information is protected. Billing tapes and printed copies of billing forms that identify the patient and contain confidential diagnostic and procedural codes are protected from unauthorized disclosure.
- If the billing staff has access to patient records or copies from them, procedures are in place to protect the confidentiality of these records and assure their proper disposal when they are no longer needed.

Physician Offices

- If physician offices are connected to the organization's computer system, security measures are in place for these offices.
- Staff members have been adequately trained on use of the system and their responsibilities for protecting confidential information.

Updated by

Jennifer E. Carpenter, RHIA, HIM practice manager
Originally prepared by: Mary D. Brandt, MBA, RHIA, CHE

Acknowledgments

Assistance from the following individuals is gratefully acknowledged:
Donna Fletcher, MPA, RHIA
Sandy Fuller, MA, RHIA
Harry Rhodes, MBA, RHIA

Issued January 2000

<
