AHIMA's Long-Term Care Health Information Practice and Documentation Guidelines

Practice Guidelines for LTC Health Information and Record Systems

---

Physical Security of Manual/Paper Records

HIM STANDARD:

- When the healthcare organization maintains all or portions of the record electronically they must have a security plan with policies and procedures that delineate how the facility will safeguard the premises, the exterior and interior of the building from unauthorized physical access and the software and equipment therein from unauthorized physical access, tampering, and theft. The software must have a method of tracking access.
- When the healthcare organization uses a manual record system they likewise must have protections of the record, including a manual record-tracking system, out guides and/or requisition slips are used consistently to indicate records removed from the files.
- When the healthcare organization maintains portions of the record electronically, a system shall be used to indicate in the paper record that specific documentation is maintained elsewhere, and how to access that documentation. Electronic access shall be granted based on assigned access privileges.
- The process for accessing manual and electronic records shall be known by employees who would have such access or may be requested to identify methods of accessing and tracking both the manual and electronic health records

Security Measures for Record Check Out-Manual

One of the most important physical security measures that must be in place in every long term care facility is a record sign-out system (log-out and/or outguides) for all types of medical records. Not only do the systems have to be in place, but they must also be enforced to be effective. Health information staff should monitor the sign-out practices and assure that records are returned promptly.

- Active Records: Outguides or a sign-out system must be in place on all nursing stations. Charts should not leave the unit without being signed out. Outguides work well because they are placed in the chart rack where the chart was removed. The authorized person who took the record must be identified along with the date and location.
- Overflow Records: Regardless of where overflow records are located in the facility, there must be a sign-out process to identify when a record has been removed, who

took the record, and where it is located.

- Discharge Records: A sign-out system must be in place when a record is removed from the health information department or record storage area.

Maintaining Security of Electronic Record Access

HIM STANDARD:

- When the healthcare organization uses electronic record access control procedures for verifying access authorization, regular review of audit logs, system activity, access reports, and security incident tracking reports are used consistently to monitor for intrusion or any unauthorized access.
- Training on the organization's electronic record security is provided to all healthcare employees empowered to request or who may receive requests to access to health records.

Facilities with electronic records or hybrid (partially electronic) records must establish policies and procedures for verifying access authorizations before granting physical access, which include documented instructions for validating the access privileges of an individual before granting those privileges. Need-to-know (Minimum Necessary) procedures for personnel access should be defined so that a user shall have access only to the data needed to perform a particular function. Need-to-know is also a criterion for removal of user accounts included in the requirements for termination procedures. Staff members should not be allowed access to information beyond the scope of their current job functions.

A computer role based access grid should be established that delineates both the access privileges and limitations based on the employee's position. Access privileges must be able to be changed as changes in the system, applications or forms are implemented or changes in access needs for individuals or classes of employees change.

Information must also be classified to indicate what level of access control is indicated.

For example:

- Public = No restrictions on access; Examples brochures, Notice of Privacy Practices
- Internal = Access by employees only, based on need to know; Examples: policies and procedures
- Confidential = Role based Access only; Protected Health Information;
- Sensitive = Role Base Assigned Access only ; HIV test results, Psychiatric or Alcohol Abuse

The **Workstation** is another integral part of electronic record physical security. HIPAA Security requires that the facility have a policy and guidelines on workstation use (documented instructions and procedures delineating the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific computer terminal site or type of site, dependent upon the sensitivity of the information accessed from that site)." Users should be guided as to unauthorized viewing. The policy might show that users need to log off when they leave the workstation unattended during their shift and before they end their shift for the day. As an alternative to logging off, password-protected screensavers could also be used to secure an unattended workstation.

The physical attributes of the workstation site must also be addressed. Some examples of this may be:

- Locking cage to enclose CPU case when left unattended
- Locking room where the workstation is located when not in use
- Protecting all removable media (e.g. diskettes, CD-ROMs, backup tapes, etc.) from unauthorized use

- Prohibiting the practice of writing down User IDs and/or Passwords where others can find and/or use them.

Workstation sites that have access to sensitive data and/or workstation sites that are in a public area may need extra physical attribute policies to maximize the security of the site. Special consideration must also be given to protection of information stored in portable devices such as laptop computers and PDAs that guard against theft, loss or unauthorized use.

Other considerations for control of physical access to electronic records include but are not limited to:

- Equipment control: Bringing hardware and software into and out of a facility and maintaining a record of that equipment including, but not limited to, the marking, handling, and disposal of hardware and storage media.
- Facility security plan: A plan to safeguard the premises and the exterior and interior of the building from unauthorized physical access and the equipment therein from unauthorized physical access, tampering, and theft.
- Physical access authorization verification: Access authorization verification must include instructions for validating the access privileges of an entity before granting those privileges.
- Maintenance records: The process for the documentation of repairs and modifications to the physical components of a facility, such as hardware, software, walls, doors, and locks.
- Personnel access need-to-know procedures: Procedures must ensure that a user has access only to the data he or she needs to perform a particular function.
- Visitor sign-in and escort procedures: Escort procedures must include procedures governing the reception and hosting of visitors, “if appropriate”.
- Testing and revision: Procedures for restricting program testing and revision to formally authorized personnel.
- Scanned documents or other specialized program of record management must have the same level of access privileges to prevent unauthorized physical access and the equipment therein from unauthorized physical access, tampering, and theft.

What to do if a Record is Lost, Destroyed or Stolen

Even with the best preventative systems in place medical records, in full or in part, can be inadvertently lost, destroyed, or stolen. To limit or minimize the harm, systems must to be in place and enforced which protect the records.

When records are lost or missing, an exhaustive search should be conducted to locate the documents or records. Once records are found, evaluate the system failure that resulted in the loss of records and implement corrective measures to prevent it from occurring again.

After an exhaustive search for lost records or in situations where the records are known to be destroyed or stolen, the next step is to reconstruct the record if possible.

Reconstruct the information by:

- Reprinting documents from any databases, such as the facility clinical computer system (MDS, care plans, etc), pharmacy (current physician orders), laboratory, and radiology databases or data backup services.
- Go to your computer backup system or your corporate server or backup of your automated document management system back (imagining, etc.)
- Retranscribe documents from the dictation system if used (check with attending physician or consultant for copies of dictated progress notes or consultative reports).

- Obtaining copies from recipients of previously distributed reports/documents, such as those sent to a physicians' offices, hospital, other healthcare facilities, or the business office.
- Obtain copies of reports generated by a healthcare facility (hospital) that relate to the resident's stay (history and physical, discharge summary, emergency room reports, etc.).
- If the current record is missing, have staff complete baseline assessments for the resident, complete a comprehensive assessment and a new care plan. Have each discipline write a summary note with the resident history and progress over the course of their stay. Verify physician orders with attending physician and have reconstructed orders signed.

If unable to reconstruct part or all of a resident's health information, document the date, the information lost, and the event precipitating the loss in the resident's record. When appropriate, document what and how information was reconstructed. Authenticate the entry as per facility policy. When information is disclosed that would have normally included the missing portion, include a copy of the entry documenting the loss of that information.

Disaster Plans

HIM STANDARD:

- A disaster plan for recovering health records damaged by fire, flood, or other destructive events in is place.
- The disaster plan includes revisions for recovering healthcare records on different types of storage media.
- The disaster plan includes provisions for a backup system, offsite access such as hosting, corporate storage and retrieval, to provide the healthcare organization's staff necessary access to health records during emergency situations.
- The disaster plan must outline alternative procedures to be utilized for continuity of care during the emergency and the procedure when there is restoration of the automated system.

Every long term care facility should have a disaster plan in place to deal with unexpected events and outline how health information/medical records will be protected from damage. A well thought out disaster plan will minimize disruption, ensure stability, and provide for orderly recovery when faced with an unforeseen event.

A plan should be in place to deal with water damage (flood, sewage back-up, sprinkler damage, etc), fire, power failures (electronic medical records and clinical information systems), resident evacuation, and other natural disasters common to your area such as a hurricane or tornado.

AHIMA has the following practice brief on disaster planning which details the steps to take in preparing for potential adverse events.

Research

- Perform a literature search on disasters and disaster planning relative to medical records or health information. Search the archives of your favorite health information listservs or Web sites. Check the Internet to see if other health organizations have posted disaster plans on their Web sites. Collect sample health information disaster plans from peers.
- Talk to colleagues who have experienced the types of disasters your facility could expect.
- Contact several fire/water/storm damage restoration companies to determine the services available in your area and obtain any instructional information they can provide. Services may include document, electronic media, and equipment restoration as well as storage. These companies can often be located in the yellow pages under

"fire/water damage restoration" or in the *Disaster Recovery Yellow Pages.*

- Determine to what extent the facility's insurance covers the costs associated with moving health information, operating elsewhere, recovering damaged information, or lost revenue secondary to the inability to restore information. In addition, determine whether your insurer offers consultation and advice on disaster planning. Many insurers provide this at little or no cost to their clients.

Drafting the Plan

- List the various types of disasters that might directly impair the operation of the facility, such as fire, explosion, tornado, hurricane, flood, earthquake, severe storm, bioterrorism, or extended power failure.
- List your department's core processes. For example, at a large hospital, the core processes might be maintenance of a correct master patient index (MPI), assembly, deficiency analysis, coding, abstracting, release of information, transcribing dictation, chart tracking, locating and provision, and generating birth certificates.

For each plausible disaster and core process, generate a contingency plan. The document might include:

- facility name
- department name
- contingency plan originator
- date
- the major function being addressed, such as chart tracking and location and provision
- the disaster being considered, such as a hurricane
- assumptions about the disaster, such as how will the disaster affect utilities; staffing and the ability of staff to report to work; security of health information and the facility itself; hardware and software; equipment and supplies; other departments; and residents presenting to the facility for treatment
- description of the existing process used for the major function being addressed
- an if/then scenario stating what will happen if a specific function cannot be performed
- inter-dependencies, such as which processes depend on the provision of certain information or services
- solutions and alternatives, including steps that can be taken to minimize damage or disruption before the disaster, ensure stability, or provide for orderly recovery
- the limitations and benefits of each solution or alternative
- activities that will need to be performed before the disaster in order to make this alternative possible, such as equipment acquisition, implementation of back-up systems, and development of disaster-related forms, materials, procedures, and staff training
- the names of the individuals responsible for performing these activities
- a list of individuals and departments with phone numbers to be contacted or notified relative to the disaster and implementation of this particular contingency plan

Implementing the Plan

- Perform the preparatory activities listed in each of the contingency plans.
- Share the preliminary plans with the facility's safety officer and risk manager.
- Develop written agreements with potential disaster recovery vendors or alternative service providers and locations as needed.
- Provide staff with the training and tools necessary to implement the plan.

- Test the plan.
- Reevaluate and revise the plan and corresponding procedures based on the input of staff, the safety officer, and the risk manager, and on simulated disaster trials.
- Include disaster training as part of staff orientation.
- Measure staff competency by asking staff to describe or demonstrate their roles and responsibilities during specific disasters. Include competencies in staff performance standards.
- Conduct drills at least semiannually.
- Review and update the plan at least annually.
- Repeat training and test competencies at least annually.

Restoring Damaged Records

In the event records are damaged in an actual disaster, contact a fire/water/storm damage restoration company. If services are contracted, the contract must provide that the business partner will:

- specify the method of recovery
- not use or further disclose the information other than as permitted or required by the contract
- use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the contract
- report to the contracting organization any inappropriate use or disclosure of the information of which it becomes aware
- ensure that any subcontractors or agents with access to the information agree to the same restrictions and conditions
- indemnify the healthcare facility from loss due to unauthorized disclosure
- upon termination of the contract, return or destroy all health information received from the contracting organization and retain no copies
- specify the time that will elapse between acquisition and return of information and equipment
- authorize the contracting entity to terminate the contract if the business partner violates any material term of the contract

To the extent records cannot be reconstructed by the damage restoration company, reconstruct the information by:

- reprinting documents from any undamaged databases, such as admission, transcription, laboratory, and radiology databases or data backup services
- retranscribing documents from the dictation system
- obtaining copies from recipients of previously distributed copies, such as physicians' offices, other healthcare facilities, or the business office

If unable to reconstruct part or all of a resident's health information, document the date, the information lost, and the event precipitating the loss in the resident's record. When appropriate, document what and how information was reconstructed. Authenticate the entry as per facility policy. When information is disclosed that would have normally included the missing portion, include a copy of the entry documenting the loss of that information.

Create and retain a record of the disaster event and a list of resident records affected, with recovery efforts, successes, and failures. This will allow for easy retrieval of general information regarding the past event should any legal or accreditation issues arise.

Post Disaster

Following the disaster, meet with staff and allow them the opportunity to:

- evaluate departmental performance and identify opportunities for improvement
- begin the grieving and healing process that may follow emotionally charged disasters

---