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

Practice Guidelines for LTC Health Information and Record Systems

Confidentiality and Release of Information

- Identification of Confidential vs. Non-confidential Information
- Resident Access to Their Records
- Confidentiality Training and Agreements with Employees and Volunteers
- Resident Identification Boards at Nursing Stations and Other Facility Locations
- Maintaining an Access/Disclosure Grid for Employees, Contractors and Outside Parties
- Handling a Request for Health Information contained in the Designated Record Set
  - Consent for Use and Disclosure of Protected Health Information
  - Redisclosure Upon Transfer to Another Healthcare Facility
- Handling Telephone Requests for Information
- Transmitting Resident Information via Facsimile
- Responding to a Subpoena or Court Order
- Removing Original Records from the Facility
- Notice of Information Practices
- Designation of a Privacy Officer

HIM STANDARD:

- The medium in which protected health information are stored, whether paper based or computer based, is the property of the healthcare organization and is maintained to serve the resident, the healthcare professional, and the healthcare organization in accordance with legal, accrediting, licensing, regulatory, and ethical standards.

- Residents’ protected health information, regardless of the medium in which they are stored, belong to the resident and are protected accordingly.

- Confidentiality policies and procedures specify that protected health information is used within the healthcare organization only for the purposes for which the data and information were collected.

- Disclosure of protected health information is restricted to those individuals who possess knowledge of applicable federal and state laws and regulations and training in the legal ramifications of subpoenas and court orders.

One of the most critical roles of the health information department is to monitor and apply regulations, professional practice standards, and facility procedures for protecting resident confidentiality, information security, and release of information. A comprehensive set of policies and procedures to comply with the Health Insurance Portability and Accountability
HIPAA privacy and security rules in regards to confidentiality and release of information must be in place in all long term care facilities. The following guidelines provide direction on common issues related to confidentiality and release of information. The guidelines take into consideration federal laws and professional practice standards, but not individual state regulations. If there is a state specific law with more stringent requirements or that allows greater privacy protections, follow the laws of your state.

Federal Regulation: 42 C.F.R. § 483.75 (4) states: The facility must keep confidential all information contained in the residents’ records, regardless of the form or storage method of the records, except when release is required by – (i) transfer to another health care institution; (ii) law; (iii) third party payment contract; or (iv) the resident.

HIPAA is a federal law that requires healthcare facilities and payers who utilize standardized transactions (such as electronic billing) to comply with the Standards for Privacy of Individually Identifiable Health Information (HIPAA Privacy Rule). The HIPAA privacy rule became final on April 14, 2001 with compliance required by April 14, 2003. This section refers to various components of the privacy rule, but does not go into full detail on all requirements. It is recommended that health information practitioners obtain a copy and review the entire HIPAA privacy rule. Copies can be obtained through the Administrative Simplification website at http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html. Additional compliance guidance regarding the HIPAA Privacy Rule and answers to Frequently Asked Questions can be located at the Office For Civil Rights website at http://www.hhs.gov/ocr/hipaa/.

Identification of Confidential vs. Non-confidential Information

HIM STANDARD:

- Residents’ protected health information is regarded as confidential and made available only to users authorized within the healthcare organization, users authorized by the resident or his/her legal representative, and users authorized by law.
- Confidentiality policies and procedures differentiate between confidential and non-confidential data and information.
- Policies and procedures address the heightened level of confidentiality provided to healthcare information related to behavioral health, substance abuse treatment, sexual or physical abuse, HIV/AIDS, abortion, and adoption.

Definition:

Protected Health Information (Individually Identifiable Health Information) is information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual that (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

The confidentiality/release of information policy should define what information is considered non-confidential and may be disclosed without a HIPAA compliant authorization and that which is considered confidential. The policy should contain information that is maintained in both paper and electronic format. State law may define non-confidential information. Federal law restricts disclosure of information related to drug and alcohol abuse treatment. Under the HIPAA privacy rule, disclosure of directory information is permitted without resident’s authorization as long as the resident has had an opportunity to agree or restrict its use. Directory information may be disclosed to individuals who ask for the resident by name. Healthcare facilities are under no obligation to disclose even non-confidential information; policies should define the facility practice. The resident population should be considered when deciding what is considered non-confidential. Special consideration may
be given to celebrities, facilities who treat HIV/AIDS residents, behavioral health facilities, etc. Under the HIPAA privacy rule,

- Non-confidential or directory information is considered to be common knowledge such as name of the resident, location in the facility (room number), their condition described in general terms (critical, stable, good, fair, transferred, treated and released, or expired), and religious affiliation (only available to members of the clergy).

- Confidential information is information made available during the course of a confidential relationship between the resident and healthcare professional. Confidential information includes – but is not limited to – all clinical data and the resident’s address on discharge. Confidential information may be disclosed only when the resident, or the resident’s legal representative, gives written authorization, or when federal or state law, subpoena, or court order requires such disclosure.

Facility policies should give direction to staff on releasing non-confidential and confidential information. Since these situations often occur at the receptionist desk or at the nursing station, staff should receive special training in dealing with requests and deciding what is acceptable to release and what is not.

Resident Access to Their Records

HIM STANDARD:

- Subject only to specific legal constraints (such as those governing minors and persons adjudicated incompetent), a resident or his/her legal representative has access to and is provided photocopies of his/her health record upon written request with reasonable notice and payment of a reasonable fee.

- Policies and procedures have been established to enable the resident to review, amend, restrict access to or correct his/her health record.

Definition:

*Designated Record Set* means (1) a group of records maintained by or for a covered entity that is (i) the medical records and billing records about individuals maintained by or for a covered health care providers; (ii) the enrollment, payment, claims adjudication, and case or medical management record system maintained by or for a health plan; or (iii) used, in whole or in part, by or for the covered entity to make decisions about individuals. (2) The term *record* means any item, collection or grouping of information that includes protected health information and is maintained, collected, used or disseminated by or for a covered entity.

By federal law, residents or their legal representative in a long term care facility have the right to access their designated record set. Facility policies should provide guidance on who is considered a legal representative based on State law (i.e. guardian, conservator, durable power of attorney, etc.) Facility procedures should also outline how each request – whether a review of the medical record or request for photocopies -- will be handled.

C.F.R. § 483.10(b)(i) states that “the resident or his or her legal representative has the right, upon oral or written request, to access all records pertaining to himself or herself including current clinical records within 24 hours (excluding weekends and holidays).” In the event the resident or the representative wants a copy of the medical records, the facility is required to make copies, after 2 working days advance notice, “at a cost not to exceed the community standard.” 42 C.F.R. § 483.10(b)(ii).

The federal regulation for nursing homes (483.10(b)(i)) requires a more stringent time frame and should be followed when acting on a request by the current resident/legal representative to access records. The HIPAA Privacy Rule timelines can be followed when responding to requests from former residents or their legal representatives.

Under the HIPAA privacy rule, the resident has the right of access to inspect and obtain a copy of their protected health information in a designated record set as long as the
information/record is maintained. The privacy rule allows facilities a longer timeframe to respond to requests to inspect or obtain copies. The facility may follow the privacy rule timeframes when responding to requests from former residents. The facility must act on the request no later than 30 days after receipt. If records or information are not maintained on-site, the facility has up to 60 days to act on the request. If the facility is unable to respond within the 30 or 60 days, the facility may have one time extension of no more than 30 days. The facility must notify the requesting party in writing of the reason/s for the delay and the date when the request will be completed. Again, the facility is only allowed one time extension.

**Steps In Handling A Request To Access/View Designated Record Set:**

When a request is made by the resident or another party to view information within the designated record set, those requests should be directed to the health information coordinator. Selecting one person or a department to handle requests will help to assure that the policy is carried out uniformly and information isn’t inappropriately disclosed or withheld.

If the requestor has the legal authority to view the record, a meeting should be set up within the 24 hours required by law for a current resident. If the requestor cannot accommodate a meeting within the 24 hour time frame, the review should be set up at a mutually agreed upon time. Since the resident or their legal representative have the right to review their records under federal law, it is not necessary to get approval from their attending physician.

Prior to the meeting, the record should be reviewed to ensure that is complete, accurate and organized. This also helps the facility to become familiar with the content and identify any potential areas of concern. Facility policy should address how to handle re-disclosure of protected health information received from another facility (i.e. hospital from a prior stay or another nursing home).

If components of the designated record set are maintained electronically in a hybrid medical record, determine how access will be provided to the electronic components of the medical record.

During the meeting, a staff member should be in attendance at all times. The staff member can be from the health information department or a designee such as nursing or social service. The staff member present at the meeting is there to answer questions and to assure that the record is not altered in any way or documents removed/destroyed. The resident/legal representative should be allowed to review and read the record without intervention from the staff member present.

If copies are requested during this meeting, an authorization to use or disclose health information form should be signed with the specific documents and dates listed. The facility’s copy charge policy should be disclosed to the resident/legal representative at the time of the request.

**Steps in Handling A Request for Copies of Designated Record Set:**

See the sections on Handling a Request for Medical Records and Copy Fees for Medical Records. The request for copies must be documented on a HIPAA compliant authorization form and signed by the resident or legal representative (for tracking purposes). The request should specifically state what records are to be copied. Review the copy fee policy with the resident/legal representative and if known, provide the estimated cost to fulfill the request before copies are made.

**Confidentiality Training and Agreements with Employees and Volunteers**

**HIM STANDARD:**

- Education and training programs provided to members of the healthcare organization as a whole and to specific departments address the confidentiality of residents’
protected health information.

- Confidentiality policies and procedures are incorporated into new employee orientations and routinely reviewed as part of each employee’s ongoing education.

- Education and training programs on confidentiality address the responsibilities of staff to protect the resident’s right to privacy and their responsibilities to safeguard protected health information.

- Confidentiality agreements are signed by everyone connected with the healthcare organization who may have access to confidential healthcare information and resident-identifiable data. It is recommended that agreements are updated annually.

- Agreements with home-based employees state that the employees assume the same responsibility as regular employees for maintaining the confidentiality of all residents’ protected health information within their control.

- Education and training programs provided to members of the healthcare organization as a whole and to specific departments address the release of residents’ protected health information.

Long term care facilities should have confidentiality training programs in place for all employees and volunteers. Under the privacy rule, training must be provided within a reasonable time after hire. It is recommended the training is reviewed annually with employees/volunteers. Training should address the employee’s responsibility in maintaining the resident’s privacy, the facility’s confidentiality and release of information policies, common situations which an employee may face which could result in a breach of confidentiality and the consequences if a breach occurs or policy is not followed. All employees should have some basic training on their responsibility. Staff members who handle requests for information should have additional training to address the situations they will face in their position.

**Definition:**

*Workforce* means employees, volunteers, trainees and other persons whose conduct, in the performance of work for a facility, is under the direct control of the facility, whether or not they are paid by the facility.

Under the HIPAA privacy rule, facilities must train all members of its workforce on their policies and procedures related to the privacy rule. The training should be based on employee’s job function and access or exposure to protected health information. All new members of the workforce must be trained within a reasonable period of time after hire. Retraining must occur when there is a policy or procedure change that affects an employee's job. In all instances, the facility must document that training was provided.

In addition to training, long term care facilities should have members of the HIPAA defined workforce – who includes employees, students, and volunteers sign a confidentiality agreement at the time of employment after they have received training. Facility policies should address the frequency for obtaining updates to the agreement (i.e. annually after training). It is not recommended that confidentiality statements/agreements be incorporated into employee handbooks where the employee signs a blanket statement at the end. It is recommended that confidentiality agreements should be separate from the employee handbook to stress the importance of maintaining resident privacy and the potential action if privacy is breached.

The following sample provides language developed by AHIMA for discussion purposes only and published in the book, Release and Disclosure, Guidelines Regarding Maintenance and Disclosure of Health Information by Mary Brandt, MBA, RHIA, CHE. It should not be used without review by your organization’s legal counsel to ensure compliance with local and state laws.

---

**Employee/Student/Volunteer Nondisclosure Agreement**

[Name of healthcare facility] has a legal and ethical responsibility to safeguard the privacy of all residents and to protect the confidentiality of their health information. In the
Resident Identification Boards at Nursing Stations and Other Facility Locations

Communication boards may be used to communicate within a facility and may contain protected health information. Common uses of communication boards include staff assignments, sharing information with other shifts, census information, etc. These communication boards that contain residents’ protected health information must be in an area that is not viewable to residents, unauthorized staff members or the public. As a general rule, the only resident communication boards that should be viewable to the public provide directory information (room number).

Maintaining an Access/Disclosure Grid for Employees, Contractors and Outside Parties

HIM STANDARD:

- With regard to access to residents’ protected health information, the healthcare organization’s and health information management department’s policies differentiate among levels of authorized users within the healthcare organization, users within the healthcare organization’s provider network, and third-party users external to the healthcare organization and its provider network.
- Contracts for services external to the healthcare organization must include business associate language that state that the companies providing the services assume responsibility for maintaining the confidentiality of all protected health information within their control.
- Policies and procedures identify when disclosure of protected health information may be made without the resident’s authorization and differentiate between mandatory disclosure (for example, reporting of child abuse) and permissive disclosure (for example, access by healthcare staff).
- Policies and procedures define those circumstances that require resident authorization prior to disclosure of information and those that do not require resident authorization.
- Policies and procedures identify those communicable diseases and other public health threats that require reporting to the appropriate governmental agency and the mechanism by which the reporting is to be done.
**Definition:**

*Minimum necessary means that when a facility uses or discloses protected health information or requests protected health information from another covered entity, the facility must make a reasonable effort to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.*

Part of the facility policies on minimum necessary and confidentiality should be an access grid that outlines which employees and contractors are considered authorized users of the information contained in the designated record set and any restrictions or limitations on what can be accessed. The grid should identify the authorized user by department and position and the limitations on access to information. If subcontractors are used for certain services (billing service, dietary, etc.) language needs to be included in the contracts outlining the employee’s responsibility to maintain resident confidentiality and their authority to access the designated record set.

<table>
<thead>
<tr>
<th>Employee/Contractor Access to Protected Health Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Position</strong></td>
</tr>
<tr>
<td>Administrator/Executive Director</td>
</tr>
<tr>
<td>Director of Nursing Services</td>
</tr>
<tr>
<td>RAI Coordinator</td>
</tr>
<tr>
<td>Staff Nurse</td>
</tr>
<tr>
<td>Nursing Assistant</td>
</tr>
<tr>
<td>Health Information Services</td>
</tr>
<tr>
<td>Health Information Consultant</td>
</tr>
<tr>
<td>Business Office Manager</td>
</tr>
<tr>
<td>Director of Laundry</td>
</tr>
<tr>
<td>Therapy Staff</td>
</tr>
</tbody>
</table>
Pastor Limited Access only to information necessary to do job and only for those residents requesting pastoral services

Receptionist No

Maintenance No

This table is not all-inclusive and is for discussion/illustration purposes only. Positions, access and scope should be determined by each facility. No recommendations are made through this illustration.

A second access grid should also be developed for access to clinical information computer systems. The grid would serve the same purpose of outlining who has access to the system and what screens or programs are available to the position.

<table>
<thead>
<tr>
<th>Employee/Contractor Access to Clinical Information Computer System</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Position</strong></td>
</tr>
<tr>
<td>Administrator/Executive Director</td>
</tr>
<tr>
<td>Director of Nursing Services</td>
</tr>
<tr>
<td>RAI Coordinator</td>
</tr>
<tr>
<td>Staff Nurse</td>
</tr>
<tr>
<td>Nursing Assistant</td>
</tr>
<tr>
<td>Health Information Services</td>
</tr>
<tr>
<td>Health Information Consultant</td>
</tr>
<tr>
<td>Business Office Manager</td>
</tr>
<tr>
<td>Director of Laundry</td>
</tr>
</tbody>
</table>
As computer systems access control becomes more sophisticated, the scope and limitation should be more specific to the specific programs and screens in the system. This table is not all-inclusive and is for discussion/illustration purposes only. Positions, access and scope should be determined by each facility. No recommendations are made through this illustration.

In addition to an access grid for employees and contractors, a grid should be included which outlines access to the designated record set by other types of providers, agencies or third-party users. This grid should outline whether an authorization to use or disclose health information form is required to be signed before information is disclosed or released and when reporting/disclosure is mandatory by law. Both federal and state regulations need to be incorporated into the facility policy and procedure and access grid.

The federal regulation (42 CFR § 483.75(4)) requires that the facility must keep confidential all information contained in the residents' records, regardless of the form or storage method of the records, except when release is required by – (i) transfer to another health care institution; (ii) law; (iii) third party payment contract; or (iv) the resident.

The disclosure grid should outline access to protected health information by the following individuals/entities and whether an authorization from the resident is required to release information.

Completion of this grid should be based on applicable federal and state laws the following are guidelines:

<table>
<thead>
<tr>
<th>Requestor or Outside Party</th>
<th>Authorization Required</th>
<th>Copy Charges Allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accrediting Agencies (JCAHO, CARF)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Attorney</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Attorney for Facility/Corporation</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Courts of Law (Court Order)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Employer of Resident</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>Family members</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Family members with demonstrated involvement in care</td>
<td>No – for verbal updates related to involvement in care</td>
<td>Yes</td>
</tr>
<tr>
<td>Federal, State, and Local Government, and Voluntary Welfare Agencies</td>
<td>No – when reporting is required by law</td>
<td>No – when reporting is required by law</td>
</tr>
<tr>
<td>Funeral Homes</td>
<td>No – when releasing remains</td>
<td>No</td>
</tr>
<tr>
<td>Health Department</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Healthcare Practitioners</td>
<td>No - for continuity of care purposes when involved in residents care and treatment</td>
<td>No – for continuity of care and continued treatment.</td>
</tr>
<tr>
<td>Healthcare Providers (hospitals, LTC facilities, home health/hospice agencies, etc.)</td>
<td>No – for continuity of care purposes</td>
<td>No – for continuity of care purposes</td>
</tr>
<tr>
<td>Insurance Companies and Third Party Payers</td>
<td>No – for third party payment purposes</td>
<td>No – for third party payment purposes</td>
</tr>
<tr>
<td>Insurance Companies for Facility/Corporation</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Law Enforcement Officials</td>
<td>Dependent on state law</td>
<td></td>
</tr>
<tr>
<td>Medical Examiner/Coroner</td>
<td>No – if reporting is required by law</td>
<td></td>
</tr>
<tr>
<td>Ombudsman</td>
<td>Dependent on state law</td>
<td></td>
</tr>
<tr>
<td>Research</td>
<td>Dependent on Research Project &amp; IRB Approval/Waiver</td>
<td>No – if project is approved by facility</td>
</tr>
<tr>
<td>Residents</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
The column “Copy Charges Allowed” should be reviewed carefully and compared to the requirements in the privacy rule and any other applicable state of federal regulations. While is may be acceptable to charge for copies, facilities may exercise discretion and judgment when determining whether or not to charge a resident, his/her legal representative or other requesting party for copies.

Handling a Request for Health Information contained in the Designated Record Set

HIM STANDARDS:

Requests for healthcare information require a valid (HIPAA compliant) authorization to disclose protected health information, unless the disclosure is required for treatment, payment or healthcare operations.

All requests for information should be handled by the health information department to assure uniform application of the facility policy and adherence to applicable laws and practice standards. When a request for information is made, the following issues should be considered before releasing information:

- Is an authorization to use or disclose health information required to be signed by the resident or their legal representative?
- What is the nature of the information requested?
- Is the information considered confidential or non-confidential?
- What is the purpose of the request?
- What is the authority of the person or agency requesting the information?
- Are there any revocations or notices to withhold information on file?

Consent for Use and Disclosure of Protected Health Information:

The HIPAA privacy rule does not require the facility to obtain the resident's consent prior to using or disclosing protected health information to carry out treatment, payment, or health care operations. The HIPAA Privacy Rule states that your facility may choose to obtain consent. The decision to obtain consent should be defined in the facility’s policies and procedures.

Redisclosure upon Transfer to Another Healthcare Facility

If the hospital or another facility's records provide important information for the continued care of the resident, those records should be sent to the next facility/agency that will be providing care. The privacy rule allows for redisclosure of resident's protected health information. Your facility should have a policy in place to ensure redisclosure is handled in a consistent manner. A LTC facility should send the most recent hospital history and physical report and discharge summary upon transfer to another facility if the information provides insight into the resident's current health status or would be beneficial in the continued diagnosis and treatment. Other documents should be redisclosed based on the content and relevance to the resident's continued care and treatment. Refer to the Frequently Asked Questions available on the Office For Civil Rights web site at http://www.hhs.gov/ocr/hipaa/ for additional information regarding this topic.

1. Unless otherwise required by state law, incorporate in your own facility’s designated record set the health information generated by other healthcare providers needed for patient diagnosis and treatment.

2. Become knowledgeable about and implement organizational compliance with federal and state laws and regulations that address redisclosure. Any redisclosure must
comply with federal and state laws and regulations.

3. Consult with legal counsel when federal and state redisclosure requirements differ and it's unclear which should prevail.

4. Develop facility policies and procedures that address redisclosure. Be sure to include the requirement that prior to disclosure, the disclosing staff member verify the authority of the person to receive the information.

5. Modify existing authorization forms to incorporate required language in the HIPAA final privacy rule.

6. In general, healthcare providers should:
   - Redisclose to other healthcare providers PHI when it is necessary to ensure the health and safety of the patient
   - Redisclose requested health information to patients when necessary, but after first encouraging the patient to obtain the most complete and accurate copies from the originating healthcare provider
   - Redisclose PHI when necessary to comply with a valid authorization
   - Redisclose PHI when necessary to comply with a legal process. Only redisclose PHI located within your legal health record (the designated record set). Note that you may be compelled by the legal discovery process to release additional individually identifiable health information if access to the information is deemed necessary for the stated purpose

7. Ask legal counsel to review draft policies and procedures prior to implementation.

8. Educate staff on new or revised policies and procedures relative to redisclosure.

9. Implement policies and procedures and monitor compliance.

10. When in doubt about a potential redisclosure, consult legal counsel.

11. When asked to certify or testify about the authenticity of redisclosed health information, state that the information was received from another healthcare facility's medical record through normal business practices, your facility received the information in good faith, and that you cannot knowledgeable speak about the record-keeping practices of the originating organization.

12. Modify existing certification forms when indicated.


Handling Telephone Requests for Information

When a request for a resident’s health information is received by telephone, the person receiving the request must decide if they have the authority to handle the request, decide whether information can be disclosed without an authorization, and verify that the individual has a right to receive the information. With the exception of requests related to the resident’s current care and treatment, other types of telephone requests should be directed to the health information management department.

Telephone requests can be honored without an authorization if they are for the purposes of treatment, payment or health care operations. This may occur when a resident’s protected health information is needed for a transfer to another health care institution (for continuity of care purposes), when required by law, for third party payment, or when requested by the resident (including the legal representative).

Regardless of the situation, if the caller’s identity is unknown, steps should be taken to verify the caller’s identity. This can be accomplished by requesting the caller’s name, address and, if applicable, company information. The facility staff member should look up the information, verify that it is accurate and return the call based on the information looked up.
Transmitting Resident Information via Facsimile

HIM STANDARD:

- Policies and procedures establish the circumstances under which transmission of resident-identifiable data and healthcare information by facsimile machine is appropriate (such as when the original document or mail-delivered photocopies will not serve the purposes of the requestor).

When the fax machine is used to release of transmit resident health information, safeguards must be in place to protect the resident's confidentiality. If a LTC facility uses the fax machine to transmit information, they must have a policy and procedure in place directing staff on the proper procedures.

- A fax cover letter must always be used when sending resident information. The cover letter should indicate whom the fax is sent to, whom it is from, the number of pages, and a confidentiality statement. A facility should never send resident information (whether medical record documents or a narrative summary/notes) without a cover sheet.

- The fax cover letter should provide specific directions on the steps to take if the fax was sent to the wrong location/person. If a facsimile transmission fails to reach the recipient, check the internal logging system of the facsimile machine to obtain the number to which the transmission was sent. If the sender becomes aware that a fax was misdirected, contact the receiver and ask that the material be returned or destroyed. Investigate misdirected faxes as a risk management occurrence or security incident; include the accidental disclosure of patient health information in the accounting of disclosures log. Mitigate the accidental disclosure and determine the need to contact the patient, organization's legal counsel, and risk management carrier.

- Preprogram fax numbers into the machine whenever possible to minimize the chance of entering an incorrect fax number resulting in a misdirected fax. Request that frequent recipients notify your facility of any fax number changes.

- Place fax machines in secure areas.

- If faxing is used to correspond with the physician and a response is needed, maintain a monitoring system to assure that a response is received. If an immediate response is needed or the resident's condition requires immediate intervention, the telephone should be used to contact the physician rather than the fax machine.

- Some type of verification process should be in place to assure that the fax was transmitted. Verification may vary from a report generated by the fax machine to a call back from the receiving party. The type of verification used should be dependent on what was sent and who it was sent to.

- Facility policy should outline the types of information that cannot be faxed. For instance, it may not be appropriate to fax highly sensitive information (HIV/AIDS status, drug or alcohol abuse information, etc.).

- Establish guidelines to address retention of information transmitted via facsimile and whether it should become part of the patient's health record (e.g., is the document part of a designated record set or a business record?).

- Take precautions to preserve the quality of faxed documents. Fax copies may fade and may need to be photocopied. Extra precautions are necessary when thermal paper is used to ensure legible copies are retained as long as the medical record is retained.

- Include in your organization's notice of information practices uses and disclosures of individually identifiable health information made via fax machine or software where appropriate (see the AHIMA practice brief "Notice of Privacy Practices").

- Obtain a written authorization for any use or disclosure of individually identifiable health information made via fax machine or software when not otherwise authorized by
the individual’s consent to treatment, payment, and healthcare operations, or federal or state law or regulation.


Responding to a Subpoena or Court Order

It is critical that state law is followed in processing a subpoena. In addition, the privacy rule has specific requirements that must be met prior to responding to a subpoena. (Refer to the privacy rule 42 C.F.R. § 164.512 (e).) The following provide general guidelines in handling a subpoena when it is received. Facility policies should be tailored to specific state statutes and the privacy rule. Generally, your facility should work with legal counsel to ensure a subpoena is valid and your facility responds appropriately.

- Check that the subpoena is signed by a representative of the court (usually the Clerk of Court).
- Determine if satisfactory assurances are received with the subpoena. Contact your facility’s legal counsel to ensure appropriate satisfactory assurances have been received or a qualified protective order is present or requested.
- If a subpoena is received notify facility administration and the facility legal counsel per facility policy. Some corporate offices require that the corporate legal department be notified and approve the release before records are sent.
- Review the entire medical record to make sure that all sections in the record are present and in the proper sequence. For a discharge record, do not make any alterations in the record or allow anyone else to make additions, corrections, or deletions after the subpoena has been received.
- If the entire medical record is requested, number the pages of the original medical record (including shingled copies), verify that the records all belong to the correct resident, and check that the resident name and medical record number are on all pages including both sides of forms. Make the requested copy after approval from administration/legal counsel if required by facility policy. Make a second copy for facility use/legal counsel.
- If the record is for a discharge resident and for litigation purposes, the records should be removed from the storage/filing area and placed in a locked location until the litigation process is complete.
- Deliver the copy of the record to the location listed on the subpoena.
- Upon return from court, write a note on the subpoena identifying by whom the subpoena was answered, the date and time, the attorney’s name, and note that a copy of the medical records was left with the court.
- If the original record is requested, contact the Clerk of Court to determine if a copy is acceptable. If the original is required for court --
- Create a Receipt for Medical Records and keep one copy for the facility and one for the person accepting the record on behalf of the court. Include on the receipt an inventory of the medical record content. For example, nurses notes – 20 pages, physician orders – 10 pages, total pages – 30.
- Place the original record in a folder with the receipt and label as the “Original Medical Record.”
- Deliver both the original record and the copy to the location listed on the subpoena.
- Remain with the original record at all times until you are sworn in.
- Request the Court Official to review the copy to see if they will accept the copy in place of the original. If the Judge or Hearing Officer refuses to accept the copy in place of the original, leave the original record. Request that the original record be returned to the facility when the case is completed.
Obtain a signature of the original copy of the Receipt for Medical Records from the Clerk of Court. Keep the original copy of the receipt.

Leave the copy of the receipt with the record held by the Court.

Upon return from court, write a note on the subpoena identifying by whom the subpoena was answered, the date and time, the attorney’s name, and that the original medical record was left with the court.

File the subpoena and the signed receipt in the resident/resident’s medical record file folder until the record is returned.

After the record is returned, check the record against the receipt to make sure that all pages are present. Reassemble the record in proper order, if necessary. Note the date returned on the receipt/subpoena and file the original record in the permanent file.

Removing Original Records from the Facility

HIM STANDARD:

- Original health records may not be physically removed except in accordance with the healthcare organization’s policies.

The original medical record should never be removed from the facility. Facility policies should specifically address removal of records and prohibit any employee, contractor or agent from removing resident medical records (in full or in part) from the facility. When records are requested for legal proceedings, it is acceptable to submit a copy of the original. If the original record is specifically requested for a legal proceeding, every effort should be made to submit a copy. For example, contact the court requesting that a copy versus the original be submitted or go to court with the original record and a copy. Request that the copy be placed into evidence rather than the original record. If the original must be placed into evidence, then the copy can be used by the facility.

If it is absolutely necessary to remove the original record, measures should be in place to physically protect the original. One possible method is to utilize the storage bags with plastic locks that can be purchased through medical record supply companies. The bag can be locked at the facility and the lock broken once at the destination. If the original record does have to be removed from the facility, it should always stay in the custody of a facility representative who takes full responsibility for its safe-keeping.

Notice of Information Practices

The HIPAA privacy rule requires facilities to provide the resident with a Notice of Information Practices also referred to as a Notice of Privacy Practices. This Notice must describe how the facility uses or discloses residents’ protected health information, the resident’s rights with respect to his/her PHI, and the facility’s legal duties under the privacy rule. The notice must be provided at the time of admission to the facility. The notice must be written in plain language and contain the following elements: (See HIPAA privacy rule for specifics under each section)

- Header: "This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please read it carefully."
- Uses and disclosures
- Separate statements for certain uses or disclosures
- Individual rights
- Covered entity’s duties (facility’s duties)
- Complaints
- Contact information
Effective date

Other optional information as described in the HIPAA privacy rule

A good faith effort must be made to obtain acknowledgement of receipt of the Notice. If your facility is unable to obtain acknowledgment, document actions taken to obtain acknowledgement and why you were unable to obtain acknowledgement.

If a resident is admitted in an emergency situation, provide the Notice as soon as reasonably practicable after the emergency situation.

The Notice must be posted in your facility; in addition, you must have copies of the Notice available for interested parties (perspective residents, visitors, family members, etc.) to have upon request.

If your organization maintains a public Web site, the Notice must be posted on the Web site.

Changes to the Notice:

- Content (material changes) to the Notice cannot be implemented prior to the effective date of the revised Notice.
- Your facility’s Notice should include a statement that it reserves the right to make changes to the Notice and how an updated Notice can be obtained. This will allow the facility to make changes to the Notice without having to redistribute the Notice to current residents. If your Notice does not contain this type of statement, it must provide an updated Notice to current residents.

A copy of each version of your facility’s Notice must be retained for six years from the date it was last in effect.

Designation of a Privacy Officer

HIPAA requires the designation of a privacy official who is responsible for the development and implementation of the policies and procedures of the facility related to the privacy rule. The facility must also designate a contact person or office who is responsible for receiving complaints related to the facility's privacy practices. The privacy official and contact person does not have to be the same individual. The rule does not require specific training or expertise.

AHIMA’s published model position description for the Privacy Officer