Fairview Health Services
Self-learning Activity

HIPAA Privacy for Caregivers

*Health Insurance Portability & Accountability Act*

Course ALL2ETH13
# Table of Contents

1. Introduction and Course Objectives ........................................ 3

2. HIPAA Review ........................................................................ 3

3. Fairview Privacy Standards for Caregivers
   A. Confidentiality of health information ................................. 4
   B. Authorization exceptions ..................................................... 4
   C. Conversations .................................................................... 5
   D. Reasonable safeguards ........................................................ 5
   E. Incidental disclosures ............................................................ 5
   F. Telephone messages .............................................................. 5
   G. Email and faxing ................................................................. 5
   H. Minimum necessary disclosure of PHI ................................. 6
   I. Sharing information with family and visitors ....................... 6
   J. Request from the Media ......................................................... 7
   K. Patient rights to access their health information .................... 7
   L. Research .............................................................................. 8
   M. Information security tips ..................................................... 8

4. Conclusion ............................................................................... 9

5. Verification of Completion ....................................................... 10
Patient Privacy and Confidentiality for Caregivers (HIPAA)

1. Introduction and Course Objectives
The Health Insurance Portability & Accountability Act (HIPAA) requires that all Fairview’s employees and volunteers understand and are trained to know how to apply privacy and security practices into their daily work with patients. At the end of this course, you will be able to:

- Demonstrate how to properly store, use, protect and dispose of HIPAA–protected information.
- Describe how to report a privacy or confidentiality concern or violation.
- Take reasonable steps to protect patient confidentiality when communicating with patients, family members, other caregivers, physicians and others, both face-to-face and electronically.

Using this self-learning activity
This document is more than just a self-learning activity. It is a reference and resource tool to help you incorporate privacy protections into your daily work. Study the materials in this packet and fill out the self-learning documentation form included at the end and return it to the Organizational Learning Department where you work. If you have a question about HIPAA privacy, ask your manager or contact Fairview’s privacy office at 612-672-5647.

2. HIPAA Review
What is HIPAA?
- Information covered by HIPAA is called protected health information (PHI). It is the demographic and health information we receive and create in the course of caring for a patient.
- HIPAA privacy is about who has the right to have access to protected health information (PHI).
- HIPAA covers PHI in all forms including electronic, verbal and printed.

HIPAA is designed to:
- Prevent the unauthorized use and release of protected health information.
- Give patients rights to access their medical records.
- Limit most disclosures of health information to the minimum necessary for the intended purpose.

3. Fairview’s Privacy Policies for Caregivers
Because you are directly involved in patient care, you will need to increase your understanding of some of the privacy standards that Fairview has adopted. Specifically, you will need to learn more about:

A. Confidentiality of health information
B. Authorization exceptions
C. Conversations
D. Reasonable safeguards
E. Incidental disclosures
F. Telephone messages
G. Email and faxing
H. Minimum necessary disclosure of PHI
I. Sharing information with family and visitors
J. Request from the Media
K. Patient rights to access their health information
L. Research
M. Information security tips

A. Confidentiality of health information
Essentially, any information that is patient-identifiable is confidential and must be protected. Only when the patient has agreed, may it be used or disclosed for purposes other than treatment or health care operations. Also, removal of the patient’s name does not mean the patient’s identity is protected; other information, such as a medical record number, a zip code or a date of birth could still be used for identification.

Remember these basic confidentiality considerations:

- **Minors**: If the patient is under age 18, a parent or guardian must be asked about the release of information for purposes other than treatment or health care operations. Exception: Minors who have consented for treatment of pregnancy or related conditions, chemical dependency or sexually transmitted diseases should be treated like an adult when it comes to releasing their health information. The parents should not receive information unless the minor has authorized us to release their information.

- **Facility Directory**: A patient has the right to restrict themselves from being included in the facility directory. This restriction can be set by the admitting department and it will prevent the patient’s name from being given to callers who ask for the patient by name. Precautions must be taken on the patient care unit to restrict visitors who are not welcomed by the patient.

- **Patient Condition**: If a patient has not restricted us from acknowledging that they are a patient, we can release their general condition or status to callers. Detailed discussions about the patient’s status should be cleared with the patient unless it is clear who is involved in the patient’s care.

B. Authorization exceptions
A valid written authorization is required for the disclosure of protected health information except in emergency situations and special cases as defined by law. Authorization exceptions include:

- Emergency care.
- Procurement organizations for cadaveric organ, eye or tissue transplantation.
- Uses or disclosures that are required by law, such as disclosure to:
  - Public health department for communicable diseases
  - Vulnerable adult or child abuse reporting
  - Health oversight agencies such as the Minnesota Department of Health
  - Agencies mandated by court order or search warrant
  - Reporting certain types of wounds (such as gunshot) or injuries to law enforcement agencies
oc. Information requested by a coroner, medical examiner, or funeral director regarding a deceased patient
oc. Information requested by law enforcement to avert a serious threat to health or safety.

C. Conversations
The privacy standards do not prohibit talking with other physicians, staff or patients as necessary to deliver health care; but, the rules do require the implementation of reasonable safeguards that are consistent with the circumstances.

D. What is a reasonable safeguard of PHI?
Reasonable safeguards include:
- Asking patients if it is OK with them before discussing their health in front of family or visitors.
- Adding curtains, screens, cubicles, dividers, shields or similar barriers to open areas where oral communications often occur between physicians and their patients or among professionals treating the patient.
- Adding a few more feet of distance between discussions and bystanders.
- Lowering your voice in public areas.
- Limiting the amount of information required on patient sign-in sheets, white boards and patient room door tags.

E. Incidental use or disclosure
HIPAA explicitly recognizes that incidental uses and disclosures occur as an inevitable by-product of necessary communications. These “incidentals” do not constitute violations of HIPAA, provided reasonable steps, such as those listed above, have been taken to limit them.

F. Telephone messages
Telephone messages may be left if reasonable safeguards are used to minimize unintentional disclosure of PHI in the messages. Because telephone messages may be heard by someone other than the patient, care must be taken not to leave any information that may disclose or imply information about specific medical treatment, tests or conditions unless it is very urgent that the patient be notified.

Example of an appropriate phone message
“This is a message for John Smith. This is Jane from the Eden Center Clinic and I’m calling to remind you of your appointment tomorrow. Please call me at 952-####-#### if you have any questions.”

G. Sending e-mails and faxes
Faxing PHI
- If you are dialing 9 to send a fax, ALWAYS use a fax cover sheet.
- The fax cover sheet should contain information on how the receiver can reach you in case the fax is sent to the wrong number.
- Be very careful as you dial. Some voice mail messages allow you to press a key to send a fax. Most health care providers have dedicated fax machines,
so if you get this type of message, you may want to redial to verify that you’ve reached the correct number.

- Fax only the minimum necessary information when possible.

**E-mailing PHI**

Sending an e-mail that contains PHI outside of Fairview is not considered a secure communication method. In other words, the privacy of a patient’s health information cannot be ensured if it is sent to an e-mail address outside Fairview, UMP or the U of M. Fairview provides encryption technology for users that send PHI via e-mail. Fairview’s *Transmission of PHI Using Electronic Mail* policy contains detailed information about the do’s and don’ts of emailing PHI, so if this applies to your job, please review this policy on the intranet.

**H. Minimum necessary disclosure of protected health information**

Minimum necessary means that the authorized release of PHI should be limited to the specific information needed to meet the objective of the request.

The *minimum necessary* requirement does not apply to care/treatment activities. However, when you, as a caregiver, are performing non-treatment activities related to your work (such as quality improvement), it is necessary that you apply the minimum necessary rule.

**I. Sharing information with family and visitors**

Working in a busy patient care setting presents special challenges. As caregivers, we want to take care of our patients, but we also want to show empathy and concern for the patient’s family members and friends.

As a caregiver, has this ever happened to you?

It is visiting hours in the hospital, you are returning from a patient’s room when you are stopped in the hall by an anxious man. “I’m looking for Steve and he is not in his room. Is he having surgery today? I’m very worried about him. We’ve been neighbors for 30 years.”

Or you work at the Elk River Institute for Athletic Medicine and Mrs. Henderson calls to ask if her husband came to his appointment today and how his therapy is progressing.

In each of these situations, these individuals are looking for reassurance as well as information. What would you say to him or her?

HIPAA allows caregivers to release some basic information *without* the patient’s prior authorization. This is considered *directory information* and includes:

- Patient’s name
- Condition
- Location in the facility
- Religion (given to clergy or community faith leaders only)
If a person asks about a patient’s condition and you’re not sure if the patient would like you to give detailed information to them, you can provide general information and refer the person to the patient or family for more detailed information.

HIPAA allows you, as a caregiver, to use your professional judgment to act in the patient’s best interest when giving protected health information to those involved in the patient’s care if the patient is unable to provide consent. If it isn’t clear that the person is involved in the patient’s care, follow these guidelines:

**Do Share:**

**General Condition**
1. “Sally had a rough night – we are monitoring her closely.”
2. “Joe had a good night – he is doing well.”
3. “Fred’s condition is serious.”

**Location**
1. “Sally transferred to the intensive care unit during the night.”
2. “Joe just got out of the operating room – he is now in the recovery room.”
3. “Fred was discharged this morning.”

**Timing or Stage in the Process**
1. “Sally is not on the unit right now but should return in about 30 minutes.”
2. “Joe should be out of recovery in approximately two hours.”
3. “Fred just left for a test and should return in an hour.”

**Don't Share:**
1. Diagnosis Information
2. Prognosis Information
3. Specific Vital Sign Information
4. Results of Diagnostic Tests (labs, radiology, etc.)

**Script for responding to questions that we should not answer:**
I’m very sorry but we cannot provide any additional information about the patient’s condition because of confidentiality laws. Please call a family member or friend of the family to obtain more information.

**J. Requests by the Media**
When the media calls, contact Fairview Media Relations at 612-672-4164 or the communications/public relations representative in your care system. All reporters and photographers must make arrangements with Fairview Media Relations before entering a Fairview facility. If you learn that a patient has contacted the media directly, contact Fairview Media Relations immediately.

**K. Patient rights to protected health information**
Patients generally have the right to review their own medical record (unless doing so would cause harm to themselves or others). Requests to review a patient’s medical record while the patient is an inpatient can completed on the patient care unit if the staff are able to accommodate the request. If staff do not have sufficient time to complete
the request, the patient should be directed to make an appointment to review the record in the HIMS department after discharge. The patient’s physician does not need to give approval prior to the patient’s review. A caregiver should be present to review the patient’s record with him/her so that questions can be answered and the record can be protected from tampering or loss.

L. Using PHI in research
HIPAA defines research as an activity that is separate from treatment, payment and operations. Under HIPAA, either the patient’s specific written authorization or a waiver of authorization from the Institutional Review Board (IRB) is required before patient information can be used or disclosed for research purposes. The use or disclosure of PHI for research subject recruitment purposes requires authorization by the patient. With specific assurances and documentation, HIPAA allows the use or disclosure of PHI without the patient’s authorization in certain situations. These situations are:

- Research using the PHI of deceased patients.
- Reviews preparatory to research.
- Research where certain identifiers are removed from the PHI.

Fairview’s Institutional Review Board is responsible for developing the appropriate HIPAA-compliant patient authorizations necessary to conduct research. Contact Fairview’s Research Administration Department (612-672-7690) or your site’s Health Information Management Department for specific questions regarding the proper use or disclosure of PHI for research purposes.

M. Security Tips
Information privacy and security go hand in hand. Be sure to follow good security habits.

<table>
<thead>
<tr>
<th>Good Security Habits</th>
<th>Bad Security Habits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log out of applications you aren’t using</td>
<td>Leave sessions logged in for others to use</td>
</tr>
<tr>
<td>Store documents on the network</td>
<td>Store documents on the desktop or hard drive</td>
</tr>
<tr>
<td>Report possible security incidents to the Technology Service Center at 612-672-6805</td>
<td>Ignore incidents because it is too much work to get involved and report them</td>
</tr>
<tr>
<td>Keep laptops and other portable devices locked</td>
<td>Leave a laptop on the front seat of your car while you are out having lunch</td>
</tr>
<tr>
<td>Delete or report e-mail spam</td>
<td>Open e-mails from unfamiliar sources</td>
</tr>
<tr>
<td>Encourage visitors and vendors to use the wireless</td>
<td>Help or allow visitors plug their laptop into a Fairview network computer jack</td>
</tr>
<tr>
<td>Use difficult to guess passwords</td>
<td>Use your spouse’s or pet’s name as your password</td>
</tr>
<tr>
<td>Access only the information needed to do your job</td>
<td>Check on the health status of your co-workers by looking in the systems you use</td>
</tr>
<tr>
<td>Good Security Habits</td>
<td>Bad Security Habits</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>Remind co-workers or report concerns when security practices are not being followed</td>
<td>Ignore co-workers bad habits</td>
</tr>
</tbody>
</table>

4. Conclusion

Additional information
If you have questions about how to apply HIPAA in your daily work, you can ask questions or get additional information by:

- Talking to your manager
- Contacting the:
  - Fairview Privacy Office by e-mail at privacy1@fairview.org or by telephone (612) 672-5647.
  - Fairview Internal Reporting Hot Line at (612) 672-2300 or (800) 530-4694.

You make a difference
HIPAA is everyone’s responsibility, from the Chairman of the Board to the volunteer delivering flowers, and each of us will be held accountable as we perform our daily tasks. You as a caregiver are on the front lines and your attention and sensitivity to patient privacy will make a positive impression on our patients.
5. Verification of Completion

Instructions:
1. Enter your personal information below.
2. Make a copy for your records.
3. Return this form to the Medical Staff Office (note: MSO keep this on file in your dept for 6 years).

NOTE: If you will use this program for renewal of your license, make a copy of this sheet for your own record keeping. It is also your responsibility to determine if this training meets the continuing education requirements of your licensing board.

Verification of completion

Program Title: HIPAA Privacy for Caregivers
Course Number: ALL2ETH13
Course Length: 30 minutes

Your Name (please print): _______________________________
Fairview Site: _________________________________________
Phone number or email: _________________________________
Date Course Completed: ________________________________

Objectives of this course:
- Demonstrate how to properly store, use, protect and dispose of HIPAA–protected information.
- Describe key Fairview policies related to HIPAA.
- Demonstrate what reasonable precautions to take to protect patient confidentiality when communicating with patients, family members, physicians and others.
- Demonstrate what to do to protect patient privacy and confidentiality.
- Demonstrate how to identify and report a privacy concern.

Instructor and Course Developer: Lois S. Dahl, MBA, RHIA; Privacy Director, Corporate Compliance, Fairview Health Services; 612-672-5650