



HIPAA EDUCATION

Dear Employee, Volunteer, Contractor, or Student:

As valued member of our workforce, we would like to take a moment to provide you with some written guidance on the federal regulation, **Health Insurance Portability and Accountability Act (HIPAA)**, implemented April 14, 2003. HIPAA may be a newer federal regulation, but confidentiality standards are not new to the healthcare industry. It's important that you understand HIPAA only builds on the fundamental standards already in place. There were elements in which we implemented new policies and procedures; however, many of our existing policies were amended to incorporate HIPAA.

HIPAA is made up of many parts; however, Administrative Simplification affects healthcare providers the most and is made up of three standards:

- **Privacy:** Establishes conditions that govern the use and disclosure of individually identifiable health information.
- **Security:** Establishes requirements for protecting the confidentiality, availability and integrity of individually identifiable health information. Implemented April 21, 2005.
- **Transaction & Code Sets:** Requires standardized transaction content, formats, diagnostic, and procedure codes. Implemented October 16, 2003.

HIPAA required facilities to:

1. Designate a Facility Privacy Official
2. Train the entire workforce
3. Create and implement facility policies and procedures
4. Identify all Business Associates
5. Implement complaint log process for patient privacy issues

Please contact any of the individuals identified below if you have any questions about this packet or HIPAA in general.

Erin Jack Facility Privacy Official (FPO) (303) 788-6088

Bobby Hollowell Local Security Officer (LSC) (303) 788-8899

Sheryl Swan Facility Identity Fraud Officer (303) 788-6040

Nursing Supervisor or Administrator On-Call, if after hours or if FPO is unavailable

Thank you for your continued cooperation and support in these important endeavors.

BASIC HIPAA OPERATING GUIDELINES

The following guidelines should assist Swedish Medical Center employees with HIPAA guidelines. As always, please use your professional judgment when making decisions related to release of patient information. Please refer questions regarding your specific department practices, as they relate to HIPAA, to your Department Director.

Internal Communication

Communication with employees and physicians on site at Swedish are not impacted by HIPAA, other than the discretion that has always been advised.

General Guideline for External Release of Information

First and foremost, an individual must be authorized to receive the requested information:

- The patient
- The patient's guardian
- The referring/treating physician
- An individual who possesses the patient's authorization to release information to them

Secondly, the information can be released if the individual can give the appropriate patient identifying information as outlined in our current "Release of Information" policy. Approved methods of identity verification are one of the following three options:

- Valid state/federal-issue photo ID (i.e., passport, driver's license)

OR

- Requestor is able to provide a minimum of three of the following items:
 - Patient social security number (required) and
 - Patient date of birth (required) and
 - Any one of the following:
 - Account number
 - Street address
 - Insurance carrier name
 - Insurance policy number
 - Medical record number
 - Birth certificate
 - Insurance card

OR

- Positive match of signature to a signature on file (i.e., request received from patient via fax or mail and signature is compared to patient signature on Conditions of Admission).

Inpatient Units – Response to Telephone Inquiries Regarding Patients

Inpatients will receive a four-digit code, which is the last four digits of their account number. They will be instructed to give this code to individuals who they feel are appropriate to receive information regarding their medical situation. Patient information should only be released to those individuals who have this code. Employees need to use their judgment when releasing information to individuals who do not have a code, as in some situations release of information will be appropriate. For example, assume a patient is admitted following a car accident and is in a coma with no family members present. An individual who calls requesting patient information and stating they are the patient's wife should receive information on the patient's medical situation if she can supply the information noted above (i.e., social security number, date of birth, etc.). She could then be given the patient's code for her use in the future.

Ancillary Departments – Response to Telephone Inquiries Regarding Patients

The "General Guideline for External Release of Information" above should guide ancillary departments in the release of telephonic information.

Faxing of Protected Health Information (PHI)

Faxing of PHI to individuals outside of the facility should be for treatment purposes only:

- To physicians' offices. If the physician is in the Meditech dictionary, the information can be faxed to his/her fax number as shown in the dictionary. If the physician is not in the dictionary, send the request to HIM (Health Information Management Department/Medical Records).
- To other healthcare providers (i.e., hospital, Skilled Nursing Facility) for emergency care only. Obtain from the provider an authorization for the release of the information signed by the patient. Confirm that the provider has the appropriate patient identifying information as noted above. Confirm fax number prior to sending.
- Other fax requests not needed for direct treatment of the patient. Send request to HIM for follow-up.

Always fax information using an approved fax cover sheet with appropriate disclaimer information.

Information Left on Answering Machines or with Family Members

We need to limit the amount of information disclosed about patients on their answering machines. The following guidelines apply:

- You may disclose you are calling from Swedish Medical Center, but do not disclose your department.
- You may leave a message with a family member or other person who answers the phone when patient is not home. Use professional judgment and limit the amount of information disclosed.
- Test results should never be left on answering machines.
- You may confirm appointments using language such as the following: "This is Mary calling from Swedish Medical Center to confirm your (or you may state the patient's name) 2:00p.m. appointment on Monday, April 14. Please call me at 303-788-xxxx if you have any questions or need to reschedule".
- If the information you are communicating is necessary to ensure quality care (i.e., pre-operative instructions – "don't eat after midnight". "take certain medications," etc.) or urgent follow-up care is required (i.e., test results require immediate action), then all information including PHI may be left on the answering machine.

Disposing of PHI

We need your help in ensuring PHI is not thrown into trash cans!! ALL PHI MUST be placed in the confidential bins for destruction. Remove labels or other patient identifying information before throwing items into the trash.

Displaying PHI

- Make sure PHI is not displayed on desks or open areas where the public could walk by and see it.
- Do not leave records on counters or areas where it is accessible to unauthorized individual.
- Offices that contain PHI should be locked.

Attendance at Meetings Where PHI is Discussed

- Individuals who have a legitimate need to know the information being discussed in order to perform their job can attend the meeting.
- The minimum necessary information should be discussed in order to accomplish the goal of the meeting.
- The information should be de-identified (removal of specific PHI) as much as is possible before being discussed.
- Students are not authorized to copy a chart or remove it from the hospital.

HIPAA POLICIES & PROCEDURES

Following is an executive summary of policies and procedures. All policies are available on Swedish Medical Center's intranet. This is only meant to summarize certain policies; you will still need to read the entire policy when it is released if it applies to your area. The policies that have been highlighted below were selected because every employee/volunteer/contractor must be aware that they exist in order to direct the patient and apply to your everyday job duties.

Notice of Privacy Practices

- SMC must provide adequate Notice of Privacy Practices to patients. This document explains to the patient how we will use his/her PHI.
- The patient must acknowledge in writing the receipt of the Notice of Privacy Practices on the Conditions of Admission/Consent for Treatment.

Opt Out of Directory (same as current confidential status/process)

- Each patient must be notified of his or her right to opt out of being listed in the Facility Directory in the Notice of Privacy Practices. A patient must request to opt out and **complete a Directory Opt Out Form** to invoke this right. Patients may opt in and out as many times as requested.
- **Forward any requests for changes in this area to Admissions.**
- If the patient opts out of the directory:
 - The patient will be made "confidential" in the Meditech directory. The confidential designation will appear as a "c" preceding the patient's name in the Patient Care Inquiry Module and the patient's PHI will not appear in the facility directory.
 - Flowers, phone calls and other deliveries will not be made unless they know exactly what room number to go to (if they ask us what room Jane Doe is in, we would **not** tell them. If they go directly to Jane Doe's room, we would not stop them).
 - The hospital will not be able to acknowledge that we have a patient by that name.

Uses and Disclosures of the Protected Health Information to Family Members or Friends for Patient Care Purposes

- The purpose of this policy is to establish a guideline for the use and disclosure of PHI, excluding information available in the facility directory, to members of a patient's family, significant other and friends. This is to safeguard patient privacy.
- During registration, admissions will give the patient a code (the last four digits of his/her account number). Patients will then use this code to give to family or friends to whom they would like us to disclose information about their care.
- When we get a call and the caller tells us the code, we should:
 - Identify his/her relevance in the patient care.
 - Discuss PHI with the caller, if appropriate.
- Nursing should still use best judgment if they think it is a good idea to withhold information or provide information when the caller does not have the code.

Management of Complaint/Grievance

- Anyone with concern about privacy breach has the right to file a complaint with the **FPO or designee** or the Secretary of Health and Human Services (HHS). The complaints and the resolution process must be made available to the Department of HHS or Office of Civil Rights, if requested.

Enforcement and Discipline

- For HIPAA-related violation, employees will be subject to corrective disciplinary action up to and including termination, in accordance with Human Resources policy. 3.03, Corrective Discipline. As they are now, Employees will still be subject to civil and criminal liability for certain violations.

Level of Violation	Example of Violation	Recommendation Action
<ul style="list-style-type: none"> Accidental and/or due to lack of proper education 	<ul style="list-style-type: none"> Improper disposal of PHI Improper protection of PHI or medical records Not properly verifying individuals by phone, in person or in writing 	<ul style="list-style-type: none"> Retraining and re-evaluation Oral warning with discussion of policy, procedures and requirements
<ul style="list-style-type: none"> Purposeful violation of privacy policy or an unacceptable number of previous violations 	<ul style="list-style-type: none"> Accessing or using PHI without having a legitimate need to do so Not forwarding appropriate information or requesting to the FOP for processing 	<ul style="list-style-type: none"> Retraining and re-evaluation Written warning/suspension - with discussion of policy, procedures and requirements
<ul style="list-style-type: none"> Purposeful violation of privacy policy with associated potential for patient harm 	<ul style="list-style-type: none"> Sale or unauthorized disclosure of PHI Any uses or disclosures that could invoke harm to a patient 	<ul style="list-style-type: none"> Termination Termination of vendor contract

Marketing

- The Marketing Department or FPO is the ONLY designee who can authorize marketing events** (this includes using patient lists for ANY communication about the hospital/events/services/treatment).
- Examples of marketing include, but are not limited to: sharing PHI with a third party for payment so third party can market home medical products or services/products of a business associate; drug company sending coupons for their products; releasing patient information to vendors to photograph newborns; or co-sponsoring community events, such as the 9 Health Fair.

Right to Restrictions

- Patients will be provided the right to request restriction of certain uses and disclosures of their PHI.
- Requests for such restrictions must be made in writing to the FPO. **No other facility employee may process such a request unless specifically authorized by the FPO.**

Confidential Communication (different than confidential status/ opt out)

- Patients will be provided the right to request Confidential Communications by alternative means or to alternative locations. Requests for Confidential Communications must be accommodated by SMC if reasonable. **No other facility employee may process such a request unless specifically authorized by the FPO.**
- Acceptable alternate means of communication include mail and telephone.
- Acceptable alternate locations include all U.S. mailing addresses and all U.S. phone numbers.
- Forward any requests for changes to Admissions to complete the Confidential communications Form.**

Authorization for Uses and Disclosures of Protected Health Information

- An authorization is required to disclose PHI to individuals outside of the facility.

Right to Amend

- Patients have the right to amend medical record information with which they disagree. The amendment does not include deleting, removing or otherwise changing the content of the record. **The request amendment must be submitted in writing to the FPO. No other facility employee may process such a request unless specifically authorized by the FPO.**

HealthONE Patient Privacy Policies

- PRI.001 Community Clergy Access to Patient Listings Under the HIPAA Privacy Standards
- PRI.002 Designated Record Set
- PRI.003 HIPAA Education in the Work Force
- PRI.004 Limited Data Set Use Agreement – Form
- PRI.005 Patient Privacy – Uses and Disclosures of De-Identified Information
- PRI.006 Patient's right to Opt Out of Being Listed in Facility Directory
- PRI.008 Uses and Disclosures of PHI to Family Members or Friends for Patient Care Purposes
- PRI.009 Uses and Disclosures of PHI for Marketing Purposes
- PRI.010 Uses and Disclosures of PHI to the News Media
- PRI.011 Verification of Requestors
- PRI.012 Business Associate Agreement
- PRI.013 Sanctions for Privacy, Security and Appropriate Access Violations
- PRI Fundraising
- PRI Patient Grievance Mechanism
- PRI Patient Privacy Monitoring Process
- PRI Releasing PHI Under the Public good Exception Policy

HCA Corporate Patient Privacy Policies

- HIM.PRI.001 Privacy Program Requirements
- HIM.PRI.002 Privacy Official
- HIM.PRI.003 Minimum Necessary
- HIM.PRI.004 Patient's Right to Access (Replaced by HealthONE Policy: Medical Records/Patient Right to Access)
- HIM.PRI.005 Patient's Right to Amend
- HIM.PRI.006 Patient's Right to Request Privacy Restrictions
- HIM.PRI.007 Notice of Privacy Practices
- HIM.PRI.008 Patient's Right to Request Confidential Communications
- HIM.PRI.009 Accounting of Disclosures
- HIM.PRI.010 Authorization for Uses and Disclosures of Protected Health Information



Acknowledgement of HIPAA Training

In order to ensure compliance with HIPAA, it is **MANDATORY** that you read the entire HIPAA Education packet provided by your Department Director. After reading the HIPAA Education packet, please complete this acknowledgement form and return it to your Department Director.

I, _____ (**print** employee/volunteer/contractor **name**) have read the HIPAA Education Packet. I acknowledge that I understand what I have read and how it affects my job at Swedish Medical Center. I also understand this form will be filed in my departmental personnel file.

If I have questions regarding the HIPAA Education Packet or HIPAA in general, I will direct them to my Department Director, who will work with the Facility Privacy Official (FPO), to provide answers to my questions.

Employee/Volunteer/Contractor **Signature**

Date

Department Name

Department Number