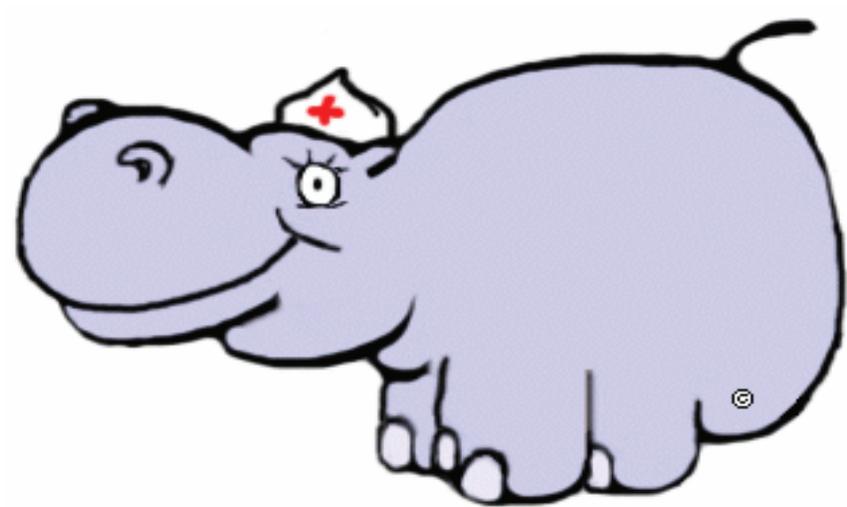


HIPAA

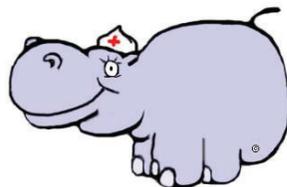
Health Insurance Portability and Accountability Act



Awareness Training for Volunteers

Southeastern Health

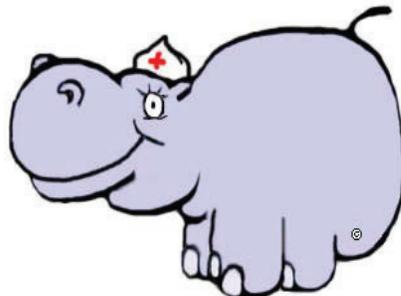
Southeastern Health has a strong tradition of protecting the privacy of patient information. Confidentiality has always been part of the hospital culture. However, now there is a new law that sets a **national standard** to protect medical records and other personal health information. It is called the **Health Insurance Portability and Accountability Act** or **HIPAA**.



Training Objectives

To have every Volunteer:

- Understand what **HIPAA** is.
- Know the meaning of Protected Health Information (**PHI**).
- Understand the significance of Treatment, Payment and Operations (**TPO**) and why it is important to remember.
- Understand what is new with **patient rights**.
- Know the **consequences** for non-compliance with the law.
- Recognize the importance of making a **renewed commitment** to patient confidentiality!!

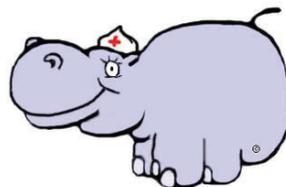


What is HIPAA?

- HIPAA is a law passed by congress in 1996.
- HIPAA sets national standards for the protection of patient information, with a compliance deadline of **April, 2003**.
- HIPAA applies to ALL health care providers: hospitals, physicians, insurance companies, labs, home care companies and surgery centers.
- HIPAA covers ALL forms of protected health information... oral, written and electronic.

Why are we, as volunteers, involved with HIPAA training?

It is everyone's responsibility to take the confidentiality of patient information seriously. Anytime volunteers come in contact with patient information (or any personal health information) written, spoken or electronically transmitted, they become involved with some facet of the HIPAA regulations! It is for this reason that the law requires awareness training for **all** healthcare personnel, including volunteers.



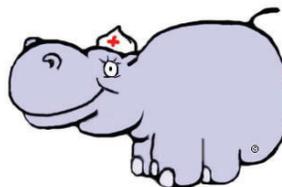
What is Protected Health Information (PHI)?

According to HIPAA **all** of the following information can be used to identify a patient:

- Addresses
- Dates
- Telephone or fax numbers
- Social Security Numbers
- Medical Records Numbers
- Patient Account Numbers
- Insurance Plan Numbers
- Vehicle Information
- License Numbers
- Medical Equipment Numbers
- Photographs
- Fingerprints
- Email addresses
- Internet addresses

This information is referred to as individually identifiable health information (IIHI). Removing a patient name from a chart is no longer sufficient to **de-identify** the patient. HIPAA refers to this information as **protected health information** or **PHI**.

Any health information that identifies someone or can be used to identify someone **MUST BE PROTECTED**.



Sharing patient information

HIPAA, under the Consent Rule, allows for the provider of care to use health information for **Treatment, Payment and Operations (TPO)**. Before HIPAA it was common to use patient information for other purposes and to share more than the **minimum necessary** information. Now patients need to give prior authorization for the use of their health information for non-TPO purposes.

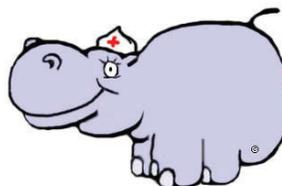
Under the **Minimum Necessary Rule** volunteers should only have access to the information they need to fulfill their assigned duties.

What is TPO?

HIPAA allows us to share patient information for:

<u>T</u>reatment	Providing care to patients
<u>P</u>ayment	Getting paid for caring for patients
<u>O</u>perations	Normal business activities such as quality improvement, training, auditing, customer service and resolution of grievances.

If use of the information does not fall under one of these categories **you must have the patient's signed authorization, before sharing that information with anyone!**



**If personal health information (PHI)
is involved**



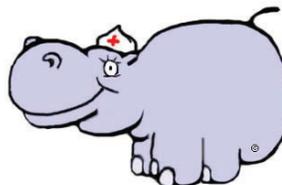
**Ask yourself -
does my sharing this information
involve **TPO** for that patient?**

(Treatment, Payment, Operations)

If the answer is **NO**

**Don't pass it along
unless you have been authorized
to do so!!**

This includes information you may see or hear about hospitalized volunteers, friends and acquaintances. Sharing information for non-TPO purposes requires authorization from the patient involved.



Scenarios

#1 During the course of your regular volunteer duties you enter a patient room to find a fellow volunteer who has been hospitalized.

OK to: Converse with the volunteer as you would normally do with other patients as part of your routine duties.

NOT OK to: Talk about the hospitalized volunteer, including sharing the information with the Volunteer Office, unless the patient has authorized the release of that information.

OK to: Mention if he/she chooses to have the Volunteer Office notified it would be best if he/she called the office directly.

#2 – You work where you have access to the patient census. While performing your regular duties you come across the name of a fellow volunteer or acquaintance.

OK to: Continue with your regular duties disregarding the information you happened upon.

NOT OK to: Assume, because he/she is a volunteer, or a personal friend, it is OK to notify the volunteer office or others you know!

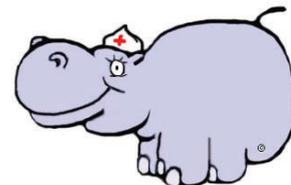
NOT OK to: Scan the census looking for people you know!

OK to: Only use patient census for minimum necessary to do your job, i.e. responding to a request for a patient room number.

#3 - You are having lunch in the cafeteria with a group of volunteer friends and someone makes the statement “Did you know that Mary is in the hospital?”

OK to: Politely stop the conversation and remind your fellow volunteer that sharing personal health information for non TPO purposes is not something we do. A reminder to all that we need to be HIPAA-Wise would be a very appropriate comment.

NOT OK to: Talk about any person’s health information, without authorization, EVEN WHEN AMONG FRIENDS.



What are the consequences of not complying with the law?

It has always been against hospital policy to improperly share, use or dispose of patient information in the wrong way. Under HIPAA, there are now fines and penalties for this.

We treat privacy seriously, which is why every volunteer and team member is required to sign a confidentiality form.

A breach of privacy may result in termination.

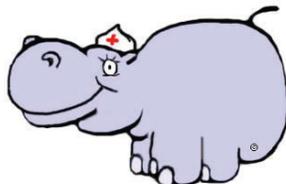
Wrongful and willful disclosure of health information carries fines and can involve jail time.

Why should we do this?

- ✓ It is the right thing to do.
- ✓ It is in keeping with the values of our organization.
- ✓ Think how you would feel if it was information about you or a loved one.

People in health care think they already do a good job protecting patient information, but HIPAA requires MORE protection.

We have to protect all health information!



What is new with Patient Rights?

Under HIPAA, patients have a right to know how their health information may be used or disclosed, and that they have certain privacy rights. These rights, some new and some revised, are communicated to our patients through a document called **Notice of Privacy Practices (NPP)**.

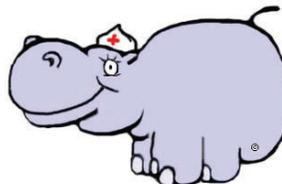
NEW rights allow patients to:

- Obtain a list of who we have shared their health information with for the past six years
- Request to amend their medical record
- Request other communications such as asking to be notified of lab results only at work and not at home

REVISED rights allow patients to:

- Review and copy their medical record
- Request restrictions on the use or sharing of their information, such as **“opting out” of the hospital directory**.

Before HIPAA, it was not uncommon for patient’s private information to be given to other companies for the purpose of **marketing products** or services. Now, HIPAA states you must get the patient's signed authorization before doing this.



Providing for the security of patient information

With Computers

We have to make sure all health information, no matter where it is, is secure. This includes information stored on computers. Everyone who uses a computer has a duty to keep health information secure.

HIPAA says we must protect all patient information on computers by:

- Properly signing-on with individual IDs and passwords
- Signing-off of computers if walking away from the desk
- Keeping IDs and passwords CONFIDENTIAL
- Protecting computer screens from unwanted viewing

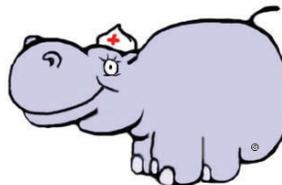
Through Proper Disposal of Information

We have to handle and dispose of patient information carefully, such as using a **shredder** instead of throwing patient information away. The procedure for the proper disposal of health information will be part of service-specific training!

RULE OF THUMB....NEVER dispose of patient information in any open area trash bin. When in doubt, ASK.

With the use of e-mail and faxes

HIPAA says we must protect all patient information transmitted electronically. Volunteers involved with these tasks will receive special training.



Reporting Violations

It is EVERYONE's responsibility to report violations, or wrong doings. Whether someone received patient information improperly, or shared patient information in the wrong way, everyone has a responsibility to report violations. When in doubt...ASK!!

Your (one-up person) department supervisor /liaison or your Manager/Volunteer Supervisor is a good place to start for answers to your questions or for reporting issues.

You can reach either the:

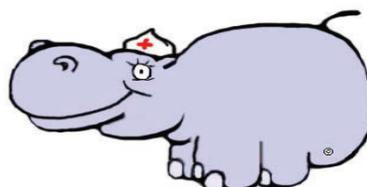
IT Security Specialist

(910-671-5684)

or

Privacy Officer/HIPAA Hotline

(910-671-5723)

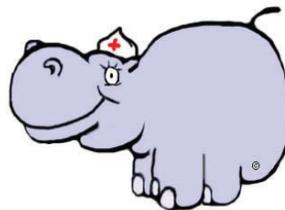


What's next?

This awareness training is intended to give you a general overview of HIPAA, and will satisfy your core training requirement. If you routinely have access to patient information, as a result of your regularly assigned duties, you will likely receive further training on how new HIPAA related policies and procedures might affect your work.

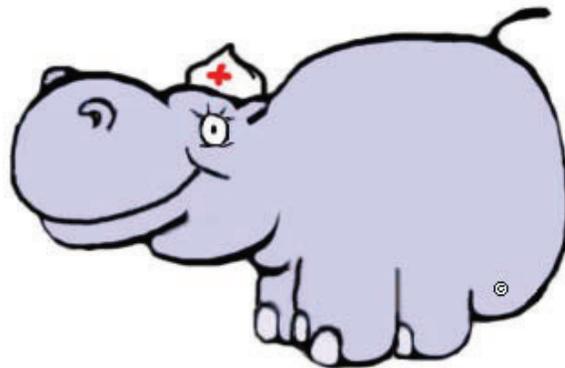
Changes will be ongoing! This is just the first phase of the act. You will be kept apprised on updates through newsletters, your service area, volunteer staff and annual education.

Help us to keep the HIPAA Awareness level HIGH!! Be HIPAA wise and model the correct behavior.



Remember to.....

- **ALWAYS STOP**, and ask yourself, should I be sharing this patient information?
- If it doesn't pertain to **TPO**, don't discuss it!!!
- Think of patient information about fellow volunteers, neighbors and acquaintances as **protected information, not for sharing!!!**
- Dispose of patient information by placing in appropriate shredding bins...**never in an open wastebasket.**
- Turn **computer screens off** if leave the station for any reason.
- **Report all abuses... enforcing the regulations is everyone's responsibility!**



I am HIPAA Wise !