

This program is designed for educational purposes only and is not a substitute for professional care. The information provided should not be used for diagnosing or treatment of a medical problem.

WARNING

The unauthorized reproduction or distribution of this copyrighted work is illegal.

Criminal copy right infringement without monetary gain is investigated by the FBI and is punishable by up to 5 years in federal prison and a fine of \$250,000



HIPPA

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT.

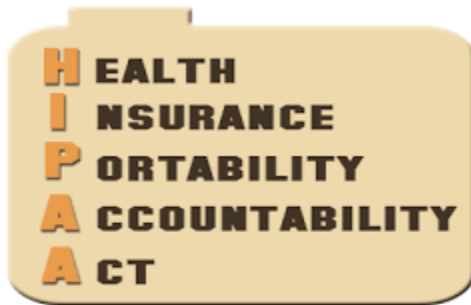
PRIVACY RIGHTS

- When you provide home care, you naturally learn a great deal about your clients' lives.
- That may make the experience more personal, but also brings with it the responsibility to keep client information private.
- **Confidentiality** or **privacy** is very important in health care.
- All health care providers , including doctors, nurses, home care providers and companions are required to keep client information private.



HIPPA AND PHI

- Privacy rights are legally enforced through **HIPAA**, a federal law passed by Congress in 1996. **HIPAA** stands for **Health Insurance Portability and Accountability Act**.
- HIPAA's Privacy Rule defines how health care providers must relate to **Protected Health Information** or **PHI**.
- **PHI** is health or billing information that identifies or can be used with other information to identify an individual.



PHI IDENTIFIERS

- patient name,
- any geographic subdivisions smaller than a state such as street address, city, county and zip code,
- dates such as birth date, admission date , discharge date, death date,
- telephone and fax numbers, email or website addresses,
- Social Security numbers,
- medical record number,
- health plan numbers or account numbers ,
- certificate or license numbers,
- vehicle ID numbers or license numbers,
- full-face photographic images or comparable images,
- finger or voiceprints,
- names of relatives.



HIPPA REQUIREMENTS

- HIPAA requires that care providers use only the **minimum amount of information** needed to give care to their clients.
- Remember that reading patient or client medical records casually or just to satisfy curiosity is a breach of HIPAA and can lead to **reprimand or job loss**.
- Always ask yourself: what is the least amount of information I need to know to do my job .
- Minimum use also applies to providing information to someone authorized to receive it.
- Again ask yourself , what is the least amount of information I need to provide to answer the request?

PRIVACY RIGHTS


- Do not discuss your patients or clients with friends, family or other clients.
- Never disclose your client's name, location or lifestyle or talk about things that occurred during your shift.
- Focus your conversation only on the client you are with.
- Never talk about other clients, their homes or any other details of their lives



PRIVACY RIGHTS

- Before your first client visit, you should know who is **authorized** to receive private information regarding your client's condition or treatment. If you don't know or if you are unsure, **check with your agency before sharing protected health information**.
- If your client wants information **withheld** from particular people, report the request to your agency's privacy officer, who will respond.
- Let your client know that you are not permitted to make decisions about restricting information.

Keeping conversations private:

- When you talk about clients to others who are involved in their care, try to prevent anyone else from overhearing the conversation.
 - Whenever possible, hold conversations about clients in private areas.
- 

PRIVACY RIGHTS

- Never give your personal cell phone or home phone number to clients.
- Clients must communicate directly with the agency about their needs rather than relying upon you as if you were a personal friend.
- You may feel very friendly toward your client, but you **must** remember your role as a **professional care provider**.



PRIVACY RIGHTS

You can share medical information about your client or patient:

- at the client or patient's doctor's office,
- at the pharmacy when picking up your client's prescriptions,
- to a supervisor or co-workers involved in that client's care,
- to 911 or the hospital,
- to a relative or friend who has authorization to receive protected health information about your client.



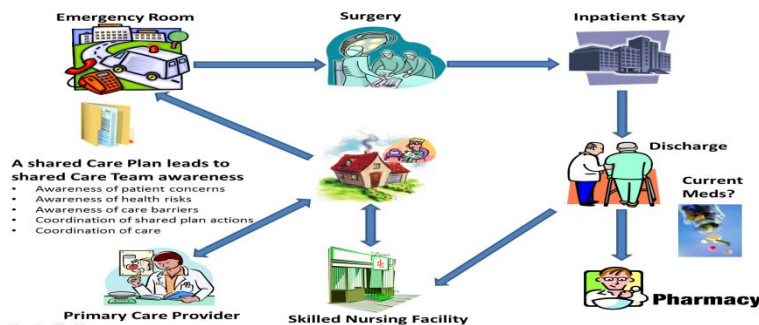
MEDICAL RECORDS MANAGEMENT

- In the office, keep client records **closed** after use, never leave any PHI on desks or open areas, including notes, labels or forms with patient names.
- When records are not in use, they should be stored in a **locked cabinet or locked room**.
- Private health information such as copies of medical records or billing records must be **shredded** or **incinerated** if it is no longer in use or needs to be destroyed.
- Any paper with PHI on it such as post it notes or scrap paper should be **shredded** as well.



CARE PLANS

- If you are seeing several clients in one day, take only the care plan or assignment sheet of the client you are visiting into the home, and leave the other records **locked** in your car out of sight.
- During your home visit, be careful not to leave private health information out where family members or others may see it.
- Any medical record should be kept in your line of sight during the visit.
- That means close to you so that you can see it at all times.



Care Plan Distribution

Electronic platform shares care plan

- Patient
- Family
- Caregiver
- Specialists
- Other involved providers

DOCUMENTING PHI COMMUNICATED BY TELEPHONE

When you give PHI to a caller authorized to receive it, you:

- document it in your notes,
- giving the name of the caller,
- the date of the call,
- a brief description of the request and information shared.



Release of Information

Documentation (cont'd)



- ▶ Why do we have to document when we release PHI (when required by law)?
 - Patients have the right to request a record of what PHI was released and to whom (Accounting of Disclosures)
- ▶ Documentation of releases of information applies to both verbal and written disclosures



© Copyright HIPAA COW

57

COMPUTER SECURITY

- When you are at the office, make sure that your computer monitor is turned away from public view to **protect client information**.
- Using a privacy filter on your monitor will decrease its visibility to others.
- Only 10% of computer security is technical;
- 90% relies upon the person who is using the computer,
- In other words, **you are the most important part of keeping electronic information secure.**



COMPUTER SECURITY

- Password protection is **essential** to computer security.
- Never share your computer password.
- Memorize your password, never keep a paper record.
- If you suspect someone has used your password, notify your supervisor immediately.
- Make sure that you log out of programs when you are not using them.
- Log off the computer or lock the computer when you are away from your workstation.



Are You
Ready for
HIPAA?



COMPUTER SECURITY

Laptops and Personal Digital Assistants:

- When using a lap top computer, keep it with you at all times or lock it safely in the car out of sight.
- One way to secure your PDA is to carry it on your body in a belly pack.
- When not in use, lock your PDA in your car out of sight just as you would lock any protected health information.



COMPUTER SECURITY

- **When faxing send only the minimum PHI needed.**
- Avoid sending sensitive health information such as information regarding HIV or sexually transmitted diseases.
- **Verify** the fax number before sending it.
- Always use a **fax cover sheet** that includes a confidentiality statement.
- Do not include any PHI on the fax cover sheet.
- Take reasonable precautions to ensure that the intended recipient is either available to receive the fax as it arrives or has exclusive access to the fax machine.
- Retrieve documents from the fax machine promptly.



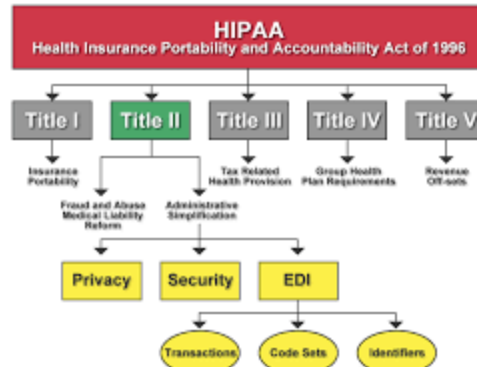
ANSWERING MACHINES

- Do not leave messages regarding private health information on an answering machine **unless** the client or patient has given you permission.



HIPAA PENALTIES

- **HIPAA violations** can result in **disciplinary action or termination** from employment.
- In addition to employee penalties, you can be subject to **civil or criminal** charges by the government.



HIPAA PENALTIES

- **Fines or prison** sentences can result from the following:
 - ✓ **Knowingly releasing** patient or client information to someone who is **not authorized** to receive it.
 - ✓ **Gaining access** to health information under **false pretenses**.
 - ✓ **Releasing** patient or client information with **harmful intent**.
 - ✓ **Selling** patient or client **information**.



THE END