Confidentiality and HIPAA

Health Insurance Portability & Accountability Act

Revised: BW/January 2016
What Is HIPAA?

- HIPAA stands for the Health Insurance Portability and Accountability Act enacted by Congress in 1996.

- This law created standards for the privacy and confidentiality of “individually identifiable” health information. This includes any information that may be used to identify a patient.
How Is Patient Information Used?

- To determine what services the patient should receive such as:
  - Treatments
  - Medications
  - Physical therapy
- Billing for the services the patient received
- Quality review to ensure good care
Who Is Authorized to See Patient Information?

- **Health Department Officials**
  - Reporting of information on communicable diseases.

- **Law Enforcement Officials**
  - Reporting of child, spousal or elderly abuse and/or information that may be used in a trial.

- **Employees involved in patient care**
Who Is Responsible for Patient Confidentiality?

All Trinitas employees, clinical AND non-clinical, are responsible for patient confidentiality.
Examples of Protected Health Information (PHI)

- Details about illness
- Information about treatments
- Photographs or videos of a patient
- Information on the patient’s chart
- Conversations between physicians, nurses and the patient
- Financial information
- Employers
- Relative’s names
Tips for Protecting Patient Confidentiality

- Do not talk about patients in public areas.
- Close patient room doors and pull the curtains when discussing health information with patients.
- Keep your voice low when discussing health information with patients or other healthcare workers.
- Never leave messages on answering machines regarding patient conditions or test results.
- Never disclose patient information to unauthorized persons, including family and friends, unless the patient has given permission.
- Do not leave patient identifiable information face-up or unattended in publicly accessible areas.
Confidentiality and Technology

- **Computerized Records**
  - Information on the computer is confidential, just like any other patient information.
  - Should be accessed on a need-to-know basis as it relates directly to the care of that patient.
How to Protect Electronic Information

- Never post passwords on monitors or walls.
- Never share passwords with anyone.
- Change your password regularly.
- Always log off the system before walking away from your computer.
- Point computer monitors away from visitors or people walking by.
- Never leave patient records in computer printers.
Dial fax numbers carefully.

Use fax transmission sheet with confidentiality statement when faxing “outside” the Hospital.

Make sure the recipient is near the receiving fax machine when the information is sent.

Never leave papers with PHI in fax or copy machines.

Always file or dispose of faxed patient information before others can see it.

All discarded PHI must be shredded or disposed of in a locked bin.
E-mail

- Never share or open attached files from an unknown source.
- Never send confidential patient information in an email unless it is encoded.
- Always double-check the address line of an e-mail before you send it.
- Never share your password or log onto the system using someone else’s password.
- Remember: e-mail is not for personal use.
Privacy Officer

- Who is the Trinitas Privacy Officer?
  - Valdery Campos (ext. 5317)
    Director – Health Information

- The Privacy Officer is responsible for:
  - Development and implementation of required policies & procedures
  - Compliance with the regulations

- Complaints regarding the use and disclosure of P.H.I. are referred to:
  - The TRMC Corporate Compliance Office:
    (908) 994-5346