ARE YOU HIPAA SAFE?

TriageLogic

WHEN PATIENTS CALL, WE'RE YOUR ANSWER ®

urac ACCREDITED
Health Call Center
Expires 04/01/2020

WHAT IS HIPAA?

- HIPAA (Health Insurance Portability and Accountability Act of 1996).
- The U.S. Department of Health and Human Services (HHS) established a set of national standards for the protection of certain health information-Called "Privacy Rule".
- These standards address the use and disclosure of an individuals health information by organizations subject to the Privacy Rule.
- They also set standards for individuals' privacy rights so that consumers understand and can control how their health information is used.

IN A NUTSHELL…

- The Privacy Act was intended to:
  1. Protects clients
  2. Reduce fraud
  3. Improve the quality of care
  4. Set strict standards for how PHI is transmitted.

WHO MUST COMPLY?

- **Health Care Providers:** Any provider of medical or other health Services that bills or is paid for healthcare in the normal course of business.

- **Health Care Clearinghouse:** Businesses that process or facilitate the processing of health information received from other businesses. Example: Companies that provide physician and hospital billing services.

- **Health Plans:** Individuals or group plans that provide or pay the cost of medical care- including both Medicare and Medicaid programs.

PENALTIES FOR NOT COMPLYING…

- Fines up to $250,000 and or civil or criminal charges including up to 10 years in jail.

HIPAA : TITLE 1 AND 2

- Title 1: Health Care Access, Portability and Renewability.
  - Designed to protect health insurance coverage for workers and their families when they change or lose their jobs.

TITLE II

- Title II : Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform. Title II is broken down into 5 rules. The 2 which are of most interest to health care providers are:
  - The Privacy Rule
  - The Security Rule

THE PRIVACY RULE

- Establishes regulations for the use and disclosure of Protected Health Information (PHI).
- PHI= ANY information about a persons health status, provision of health care, payment, and medical records- Basically ANYTHING that identifies an individual.

EXAMPLES OF PHI

- Name
- Address
- Name of relatives
- Name of employers
- Date of Birth
- Telephone Number
- Fax Number
- Email Address
- Social Security Number
- Health Plan Number
- VIN numbers
- License Numbers
- Account Numbers
- URL
- Finger or voice prints
- Photographic images
- "any other unique identifying code or characteristic".

THE PRIVACY RULE

- Requires that providers keep a record of all disclosures.
- Providers must chart their interactions with others.
- Have/use release of information forms
- Make privacy policies and procedures available upon request.

THE SECURITY RULE

- 3 specific types:
  - Administrative
  - Physical
  - Technical

ADMINISTRATIVE SAFEGUARDS

- These are policies and procedures that show how a practice will comply with HIPAA (TriageLogic Policy and Procedure Manual)

PHYSICAL SAFEGUARDS

- Physical Safeguards are those expectations to physically monitor any inappropriate access to protected data.
- This part of the Rule says that hardware and software must be introduced safely and be removed properly.

OFFICE SPACE MUST BE SECURE ALSO

- Office space must also be a physical safeguard. Steps you should follow:
  - make sure your computer screen faces away from where persons might see your screen
  - lock your screen if you walk away from your computer
  - do not give anyone your passwords
  - minimize your screen if someone walks into your office.
  - Do not allow others to utilize your work computer.
  - Work in a quiet environment with a door so you can block out "home noise".

WAYS TO STAY COMPLIANT…

- Always: be aware of where you are, who is around you and what information can be seen or heard. Take reasonable measures to minimize the chance of incidental disclosures to others.
- Don't: Browse through a patient's chart/note or other files out of curiosity. Access only the portions of the medical record that you need to perform your specific role.

INCIDENTAL DISCLOSURES

- **Incidental Disclosure**: generally refers to a sharing of PHI that occurs related to an allowable disclosure of PHI.

  An "incidental disclosure" is allowed if steps are taken to limit them.

  - *For example, visitors may hear a patient's name as it's called out in a waiting room or overhear a clinical discussion as they are walking down a hallway on the unit.*

IF PROTECTIONS ARE IN PLACE:

- You can talk about patient conditions in our education programs.
- Prescriptions can be discussed with the patient by phone.
- Messages can be left on answering machines or with those who answer the phone, but the message should be limited to minimum necessary and sensitive information should not be used.

ELECTRONIC COMMUNICATION

- Faxes, emails and computer printouts may contain patient information.
- Never send PHI over an unsecured method.
- No PHI should EVER be emailed.
- Designated individuals have authority to print PHI and they must have a crisscross shredder available and immediately shred the information as soon as they are finished using it.

WRITTEN PERMISSION IS NOT NEEDED

- As required by law, such as reporting abuse or neglect.
- For law enforcement.
- For organ donation organizations.
- To medical examiners and funeral directors.
- To avoid threats to health and safety.
- For certain research activities if the IRB has granted a waiver.

PATIENT RIGHTS

- **The Privacy Rule gives patients the right to:**
- have their PHI protected.
- inspect and copy their records.
- request that PHI in their records be corrected or changed.
- ask for limits on how their PHI is used or shared.
- ask that they be contacted in a specific way, such as at work and not at home.
- get a list of disclosures made of their PHI.

OUR RESPONSIBILITY

- **Anyone that works with PHI is legally and ethically responsible and accountable for maintaining the privacy and confidentiality of protected health information (PHI).**

POST TEST

TRUE OR FALSE?

- A patients email address is **NOT** HIPAA protected information?

FALSE…

WHICH OF THE FOLLOWING IS NOT A WAY TO ENSURE SECURITY

A. Keeping your computer screen tilted away from public areas

B. Locking up laptops and other portable devices when not in use

C. Leaving a shared computer logged on, so your coworker doesn't have to log on all over again

D. Selecting secure passwords

E. Making sure doors and desks are locked as appropriate

C. Leaving a shared computer logged on, so your coworker doesn’t have to log on all over again

WRITTEN PERMISSION IS NOT REQUIRED WHEN REPORTING ABUSE OR NEGLECT?

- TRUE or FALSE?

- TRUE

HOW CAN YOU PROTECT PHI IN YOUR OFFICE SETTING?

1. Make sure your computer screen faces away from where persons might see your screen
2. Lock your screen if you walk away from your computer do not give anyone your passwords
3. Minimize your screen if someone walks into your office.
4. Do not allow others to utilize your work computer.
5. If working from home, work in a quiet environment with a door so you can block out “home noise”.