HIPAA and You

The Basics

The Purpose of HIPAA Privacy Rules

1. Provide strong federal protections for privacy rights
   - Ensure individual trust in the privacy and security of his or her health information

2. Preserve quality health care
   - Encourage open communication with providers

3. Assure that the right information is flowing to the right people at the right time
   - Patient Trust Must Be Maintained. The most important consequence of violations is that we may lose our patients' trust.

What Does This Training Mean to Me?

You are expected to be able to:

- Recognize PHI that requires protection. PHI is **P**rotected **H**ealth **I**nformation.
- Determine when it is permissible to access, use or disclose PHI, and
- Reduce the risk of impermissible access to, use or disclosure of PHI.

Privacy Rule Provision

The privacy rule covers PHI :

1. PHI includes all information that identifies an individual:
   - For example, patient name, date of birth, contact information, social security number, age, and diagnosis.
   - Any aspect of information that identifies an individual is considered confidential, including information that relates to a past present or future medical condition, the actual provision of health care and past, present or further payments for health care.
   - For more on HIPAA identifiers see Appendix
2. PHI is more than the Medical Record information. It also includes:
   - Written communications, memos, emails
   - Patient stamper plates
   - Electronic forms
   - Verbal conversations
   - IV and medication labels
   - X-rays, monitors, EKGs, etc

Privacy Rule Provision (con't)

Use and sharing of patient information

- Can be used and shared for purposes of treatment, payment, or business operations without a patient's express permission or consent. In other words, as a healthcare provider you can freely share information for treatment purposes without a signed patient authorization.
- If patient information is going to be used for marketing, advertising, or other purposes, the patient/individual **must** express permission (authorization/consent) .

Privacy Rule Provision (con't)

Minimum necessary rule

- In general, access to protected health information is always based on "need to know" basis. Only the "minimum necessary" PHI should be used or disclosed for the purpose at hand.
- Individuals needing to know/access PHI are those:
  - providing care and treatment
  - performing payment/billing activities
  - participating in of healthcare operations
- When friends and family ask for information:
  - Clinical staff may disclose information to family or friends directly involved in the patient's care—as long as the patient does not object.
  - Patients identify the individuals directly involved in their care who may be provided information.
  - Please note that when a health care provider is allowed to share a patient's health information with a person, information may be shared face-to-face, over the phone, or in writing.

Preventing Breaches of PHI :Physical Security

Resist the temptation to peek

- No matter how curious you might be regarding the health of a coworker, a friend, a celebrity, or a family , member, do not access a medical record unless you are authorized to do so.
- Never access or discuss a fellow employee's PHI unless it is for purposes allowed by law and required for your job.

Screen PHI from public view

- Restrict patient information to those who have a "need to know."
- Shield the key strokes when entering an access code to prevent others from seeing the code.
- Never leave patient charts or computer screens open to the public view.
- Never Leave Medical Information Unattended

Think Twice When You Talk About PHI

- Confidential Conversations should be held in a private area whenever possible. Never hold conversation about patients in public areas (elevators, restrooms, hallways, etc.),including talking on a phone where others may overhear.
- Confidential information should always be discussed in private.
- Lower your voice when you must share PHI in areas where others might overhear.
- If possible, close the door when consulting with patients and/or family members or when dictating.
- Be sure to ask the patient in advance if it is acceptable to speak with his or her family members.

Double Check Forms

- Check to make sure that you are giving the correct paperwork to the right member or patient.
- Examples include: after-visit summaries, discharge instructions, and pharmacy inserts. Many incidents are paper related and preventable.

Preventing Breaches of PHI :Physical Security

Prevent Unauthorized Access to Facilities and Secure Areas

- If you are in a restricted area and notice there is someone you do not recognize, notify your supervisor. Also, ask the individual, “May I help you?” or say, “You seem to be lost”, and then direct them to where they need to go or refer them to management. badge
- Keep doors locked and restrict access to areas where sensitive information or equipment is kept.
- Do not allow others to “tailgate”, or follow you into a restricted area. enter restricted areas, or otherwise be directed to management.
- If applicable, turn in your badge and keys to your supervisor when you leave permanently leave RotaCare employment.

Disposing of PHI

- Never dispose of paper or items containing patient information in the regular trash. Remember-PHI is not only paper! (Includes blue stamper plates too).
- Ask yourself, “Does this include patient information?” If the answer is yes, then it doesn’t go in the regular trash.
- When paper items include patient information, they should be disposed of in department shredding boxes. Non-paper items should be destroyed in other ways.

Preventing Breaches of PHI: Technical Security

- Never share your computer password with anyone or log on to a computer for someone else to use.
- Logout or use secure screensavers when leaving computer unattended.
- Never expose patient PHI on social media (Facebook, Twitter, Instagram, etc.)

Preventing Breaches of PHI: Faxing of Information Considerations

When Is Faxing Appropriate?

- PHI is needed urgently for patient care or to obtain payment
- It is authorized by the patient/legal representative

When Faxing PHI:

- Always consider security of information, be alert, and decide when faxing may not be the best method of delivering PHI.
- If a fax contains PHI, first determine if specific or additional authorization is required.
- Ask yourself, “Is the information necessary in order to facilitate patient safety, treatment, healthcare operations or continuity of care?”
- Verify that the recipient has the authority to receive the information.
- Never fax more than the minimum amount of information necessary to facilitate patient safety, treatment, healthcare operations and continuity of care.

Preventing Breaches of PHI: Faxing of Information Considerations (con't)

Apply Faxing "Best Practice"

- Verify the accuracy of fax numbers before sending
- Pre-program frequently called numbers to cut down on dialing errors; send a test fax and verify receipt
- Notify others if your fax number changes
- Ensure your fax machine is in a secure location
- Do not let faxes sit on the machine for extended periods of time; provide a means of sorting incoming faxes until they can be picked up.
- Do not read fax communications that are not intended for you.
- Remember to ALWAYS use a cover sheet. Cover sheets are required for all transmissions
- If patient medical records are being faxed, include the standard Disclaimer/Warning developed by the organization.

If a misdirected fax containing PHI occurs this is considered a disclosure of information and may present significant risk. If this happens, do the following:

- Immediately transmit a request to the unintended receiver requesting that the material be destroyed immediately or returned by mail. Save documentation of this transmission.
- Obtain the correct fax number of the intended recipient and re-transmit.
- Complete an Occurrence Report and Follow facility procedures

Steps for Creating a Culture of Compliance

1. Treat protected health information (PHI) as if it were your own
2. Access only information needed to do your job
3. Before leaving at the end of your shift, empty your pockets. Never remove patient information from the facility. Never take patient information home or leave it in a locker or unsecured place.
4. Report any violation of privacy protection, violations include:
   - Failure to comply with privacy policies and procedures and federal regulations.
   - Wrongful access, use and disclosure of protected health information
   - Failure to safeguard patient's health information
5. Reporting leads to improvement of our privacy practices. Report suspected violations or concerns. There will be no retaliation against individuals for reporting suspected privacy violations in good faith. The important thing is to report your concerns so the problem can be corrected as soon as possible.

Resources

- Office for Civil Rights (OCR):
  - www.hhs.gov/ocr
- Office of the National Coordinator
  - http://healthhiy.hhs.gov
- http://www.medscape.org/viewarticle/762170_slide
- Kaiser Permanente, HIPAA 101: Privacy & Security Basics

Appendix

There are 18 HIPAA Identifiers

"HIPAA identifiers" means any of the following identifiers, either of the individual or of his/her relatives, employers or household members:

(1) Names

(2) All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (a) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (b) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000

(3) All Date elements (except year) for dates directly related to an individual, including of birth date, an admission or discharge date, date of death; and all ages over 89 and any date (including year) indicative of such age, however such ages and elements may be aggregated into a single category of age 90 or older.

(4) Telephone numbers

(5) Fax numbers

(6) Email addresses

(7) Social Security Numbers

(8) Medical record numbers

(9) Health plan beneficiary numbers

(10) Account numbers

(11) Certificate/license numbers

(12) Vehicle identifiers and serial numbers, including license plate numbers

(13) Device identifiers and serial numbers

(14) URLs

(15) Internet Protocol address numbers

(16) Biometric identifiers including finger and voice prints

(17) Full face photographic images and any comparable images; and

(18) Any other unique identifying number, characteristic, or code (provided that (a) the code or other record identifier is not derived from or related to other information (for example scramble MRNs and SSNs are not permitted) and not otherwise translatable to identify the individual; (b) the covered entity does not use or disclose the code or other record identifier for any other purpose; (c) and the covered entity does not disclose the mechanism for re-identification