HIPAA Privacy and Security Training

Please read through these slides and there will be a short 5 question quiz at the end verifying your understanding of the UDPT HIPAA Policy
HIPAA Privacy and security Training

• The University of Delaware Physical Therapy Department’s Clinical Services is providing this training about maintenance of patient privacy through the proper handling of our patients’ protected health information as required under the Health Information Portability and Accountability Act of 1996 (HIPAA).
HIPAA Privacy Rule Overview

• The Privacy Rule creates national standards to protect an individual’s medical records and other health information, but will not interfere with a patient’s access to, or the quality of health care delivery.
  • It gives patients more control over their health information.
  • It sets boundaries on the use and release of health records.
  • It requires that Providers must have appropriate safeguards to protect the privacy of health information.
  • It holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights.
  • It strikes a balances when public responsibility requires disclosure of some Protected Health Information to protect public health.
• More restrictive state regulations will still supercede the Privacy Rule.
For patients, the Privacy Rule means being able to make informed choices when seeking care and reimbursement for that care.

• It enables patients to find out how the Provider might use their information, and also what disclosures of that information have been made to other parties.
• It generally limits release of information to the minimum reasonably needed for the purpose of disclosure.
• It gives patients the right to examine and obtain a copy of their own health records and request corrections.
HIPAA Security Rule Overview

• The Security Rule is designed to protect electronic health information.
  • This includes information stored on hard drives, removable or transportable digital memory medium, and information transported via the Internet, email, or other means.
  • It DOES NOT cover fax or voice telephone transmission
Some HIPAA Terminologies

☒ **Covered Entity (CE)** – Health Care Providers, Health Plans, or Clearinghouses (All must comply with HIPAA.)

☒ **Protected Health Information (PHI)** – Any patient information transmitted or maintained by a CE

☒ **Privacy Notice** – Specifies all of the uses and disclosures that a Provider will make of the patients PHI
What is PHI (Protected Health Information)?

• **Names** - Individual, relatives, employers or household members of the individual

• **Geographic identifiers** - Subdivisions smaller than a state, street address(es), City, County, Precinct

• **Zip codes** - at any level other than the initial 3 digits (e.g., NNNXX-XXXX). Geographical areas of 20,000 or less must be reported as 000.
PHI

跷 All date elements - Birth date, Admission date, Discharge date, and Date of death. All ages over 89, including year are considered personal identifiers (such ages and elements may be represented in aggregated reporting as single category "age 90 or older").

跷 All Billing Details - any information about the payments for services, insurance follow-up, collection notes, etc.
• **Personal numbers** - Telephone numbers, Fax numbers, Social security numbers, Medical Record numbers, Health plan beneficiary numbers, Account numbers, Certificate/License numbers, Vehicle identifiers and serial numbers (including license plate numbers), and Device identifiers and serial numbers.
PHI

- **Web identifiers** - Electronic mail addresses, Web Universal Resource Locators (URLs), and Internet Protocol (IP) address numbers
- **Biometric identifiers** - including finger, iris and voice prints
- **X-rays, Full-face photographic images** and any comparable images,
- **Any other unique identifying number, characteristic or code**
HIPAA Privacy & Security Requirements

• Covered Entities must:
  • Ensure confidentiality, integrity, and availability of all PHI that the organization creates, receives, maintains or transmits.
  • Protect against all reasonably anticipated threats, hazards or unpermitted disclosure of said information
Clinical Procedures for PHI

• While a patient is present, printed materials and laptops are to be in the hands of a therapist when possible

• If a laptop is placed next to a patient while a therapist is treating, the chart is to be placed face down so that all identifying information is not visible

• Patients may not be left unattended at the island counter
Clinical Procedures for PHI

• Patient printed information is to be returned to student/therapist bins when not immediately being accessed.

• At the end of the day, the last therapist to leave will lock the Clinic Office door.
Administrative Procedures for Protecting PHI

• PHI at the front desk and in the billing area cannot be available for other patients viewing
• While conducting conversations about PHI, care must be taken to speak in low tones
• Intercom system must be used to communicate about calls and PHI
• When using a computer, use your unique sign-in and password. NEVER give your password to anyone. Do not remain logged in when you are away from your work station.

• Use common sense security. Make sure doors and desks are locked as appropriate.

• Never leave printed information or anything containing PHI out for others to see or copy.
• Any concerned individual may lodge a complaint concerning privacy issues without fear of reprisal. Such issues could include, but are not limited to, allegations that:
  - PHI was used/disclosed improperly
  - Access or amendment rights were wrongfully denied
  - The Facility's Notice of Privacy Practices does not reflect current practices accurately.
• Any patient wishing to lodge a complaint must be given a "Complaint Form" as quickly as possible

• Any patient that expresses a desire to exercise their rights as outlined in the "Privacy Rule", involving their PHI must be given the appropriate form or referral to the Privacy Coordinator as quickly as possible.
• Until further notice, the Business Manager will serve as the Privacy Coordinator.

• At the end of each day, the Front Desk Representative will be responsible for checking to see that all bins, file cabinets and doors are locked that contain PHI.
Avoiding someone’s name is NOT Enough

• You CANNOT Speak about a patient or their condition outside of the clinic
  • This means you cannot describe their injuries, their job, etc. This is all protected health information- when the collective info clearly describes an individual- just because you do not use the name does not mean you are following HIPAA guidelines
REFRAIN from speaking about patients outside the clinic setting

• For example, “an English professor with an ACL injury” easily could identify that individual here on campus- or a “volleyball player with a fracture”, even saying “A patient at UDPT I saw today with a lung transplant” in a clinic this size is a violation as we may have only one patient of that type so their identity could easily be discovered from your info- any sharing of that information is a violation of HIPAA
This is Serious- If you cannot comply we cannot provide you a spot here at UDPT

• We appreciate all of you who respect patient’s privacy and know at times it can be difficult to keep from sharing information you learned on the floor or things you see- especially when you are excited about this profession.

• Please note- if you need to talk to someone about something you are seeing or experiencing here at UDPT- talk directly to the supervising PT’s. We are happy to help you understand what you are seeing/experiencing here in the clinic.
Quiz

Please mark your answers in the space provided on your checklist
What does HIPAA stand for?

A. Health Insurance Privacy and Accessibility Act
B. Health Information Portability and Accountability Act
C. Health Insurance Portability and Accessibility Act
D. Health Insurance Privacy and Accountability Act
Question #2

Which of the following are true statements about the Privacy Rule?

A. It does not establish safeguards that providers and others must achieve to protect the privacy and safety of health information

B. It holds violators accountable with civil and criminal penalties

C. It lets Providers share health information with any other Provider for any reason

D. It gives patients less control over their information
Question #3

What does PHI stand for?

A. Personal Health Instructions
B. Protected Health Information
C. Private Health Instructions
D. Personal Health Information
Question #4

Which one of the following is NOT Protected Health Information?

A. Computerized memory containing patient reports
B. A hospital bill
C. Zip Code
D. Research data that doesn’t contain any information that identifies the individual
Question #5

Which of the following is NOT covered by the Security Rule?

A. USB Drives
B. Faxes
C. Hard drives
D. CDs
***BRING ANSWERS TO YOUR FIRST DAY***

Printed Name: __________________________________________

Signature: ______________________________________________

Date: ___________________________________________________

* Write Down your answers to the HIPAA Quiz:

1) ______ 2) ______ 3) ______ 4) ______ 5)_______

* There are 11 HIPAA violations in the pictures below. Please circle one and indicate the corresponding number. The first one is done for you.
Illustration portion of Quiz

• Circle the part of the picture that illustrates the violations below. Draw a line from the circle and indicate the corresponding number. The first one is done for you. Complete the worksheet by matching the violations in the following slides with illustration. Circle each violation and indicate the corresponding number.

• Continue to next slide for list of violations
Answers to HIPAA Illustration Quiz

• 1. Notice of Privacy Practices is not posted in a high traffic area.
• 2. The fax machine, located in the lobby/reception area where patients pass through, is left unattended with confidential pages falling out.
• 3. A doctor and nurse are talking about a case within ear’s shot of a patient
• 4. A patient is peering over the reception counter with an easy view of the computer that contains confidential information.
• 5. Blood vials are left unattended and some are unlabeled.
• 6. Trash can contains medical records in a lobby area where patients walk.
• 7. Patient is left alone in an empty doctor’s office.
• 8. Computer in the doctor’s office is left on with confidential information on the screen.
• 9. Medical records are stacked on the doctor’s desk next to where the patient is sitting.
• 10. Waste basket in the doctor’s office contains medical records.
• 11. The door to the reception area is left open.