HIPAA Training

Nebraska Methodist College of Nursing and Allied Health
What is HIPAA?

• “HIPAA” is the Health Insurance Portability and Accountability Act of 1996.

• HIPAA is a federal law that specifies the basic requirements “covered entities” must follow to protect the security and privacy of personally identifiable health information (“PHI”).
Why is HIPAA important?

- Patients expect:
  - Privacy and freedom from intrusions or disturbances regarding their personal affairs.
  - All communications and records concerning their healthcare will be treated as confidential.
  - Patient information will be shared only with those who need to know the information to perform their duties on behalf of the patient.
  - We will use utmost care and sensitivity when using or sharing information relating to our patient’s health care.
Key HIPAA Terms

- “PHI” means personally identifiable health information.
- “Covered Entities” mean those entities bound to follow HIPAA and includes both health care providers and payors.
- “BA” or “Business Associate” is a person or company that performs a service on behalf of a Covered Entity and is contractually bound to follow HIPAA.
Who is covered under HIPAA?

- Under HIPAA, all Covered Entities must comply with the HIPAA Privacy and Security Regulations.
- A Covered Entity includes:
  - A health care provider who transmits any health information in electronic form;
  - A health insurer/insurance plan; and
  - A health care clearinghouse.
- The HIPAA rules apply to all of a covered entity’s workforce, including NMC students and faculty!
What is Protected Health Information ("PHI")?

- PHI includes all individually identifiable health information relating to a:
  - Person’s past, present and future health or condition;
  - Provision of health services to the person;
  - Past, present and future payment of health services to the person...and
  - Any information that identifies the individual or for which there is a **reasonable basis to believe it can be used to identify the individual**.
When does the HIPAA Privacy Rule apply?

The HIPAA Privacy Rule applies to all PHI in whatever form or however it may be transmitted:

- Electronically
- Paper
- Orally
What does the HIPAA Privacy Rule say?

A Covered Entity cannot use or share PHI without the patient’s prior written consent except for:

- Treatment
- Payment; or
- Health Care Operations
Your Responsibilities under HIPAA:

- Respect the patient’s right to privacy
- Know the hospital and clinic’s privacy policies
- Be sensitive
- Only use or disclose PHI for work or education related purposes on a need to know basis
- Curb human nature . . .
  - Resist curiosity / Don’t share!
Patient rights under HIPAA...

- **Right to Receive a Privacy Notice:**
  - The Privacy Notice describes –
    - How PHI is used and disclosed by an organization
    - How the patient may access and obtain a copy of their medical records
    - A summary of patient rights under HIPAA
    - How to file a complaint and contact information for filing a complaint
Patient’s rights under HIPAA (cont.):

**Right to Access:**

- Patients have the right to:
  - Access or inspect their health record
  - Obtain a copy of their health record from their healthcare provider
  - Request restrictions on most uses of their PHI other than for treatment, payment, or health care operations
Patient’s rights under HIPAA (cont.):

- **Right to Amend:**
  - Patients have the right to request an amendment (clarification or challenge) to their medical record.
    - The patient must make the request in writing
    - The provider will review and determine if they agree or disagree with request
    - Request for Amendment becomes part of permanent record.
Patient’s rights under HIPAA (cont.):

- **Right to Accounting of Disclosures**
  - Patients have the right to request a list of when and why their confidential information was released.
    - Patients may request a list of disclosures/releases for the past six years (starting in April 2003) including:
      - Date of disclosure
      - Name of person or entity who received information and address if known
      - Brief description of reason for disclosure
  - **Exceptions**: Covered Entity is not required to list disclosures made for treatment, payment, or healthcare operations or pursuant to a patient authorization
Patient’s rights under HIPAA (cont.):

- **Right to Request Restrictions:**
  - The patient has the right to request that a Covered Entity restrict the use and disclosure/release of their PHI.
    - The Covered Entity is not required to accept a request for restriction(s).
  - Patient can also request to receive communications by alternative means or locations.
    - The Covered Entity must agree to requests for alternate methods of communication unless it is unable to comply.
De-Identifying PHI:

- If information is “de-identified,” you can share it freely without restrictions under HIPAA.
- However, to de-identify PHI under HIPAA, you must remove any and all of the 18 elements that could be used to identify the individual or the individual’s relatives, employers, or household members.
Health information is considered “identifiable” if any of the following are present:

1. **Names** (i.e. patient’s initials)
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, 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.
   b. The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000.
3. All elements of **dates** (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
Health information is considered identifiable if any of the following are present: (cont.)

4. Telephone numbers.
5. Facsimile numbers.
6. Electronic mail addresses.
7. Social security numbers.
8. Medical record numbers.
9. Health plan beneficiary numbers.
10. Account numbers.
12. Vehicle identifiers and serial numbers, including license plate numbers.
15. Internet protocol (IP) address numbers.
16. Biometric identifiers, including fingerprints and voiceprints.
17. Full-face photographic images and any comparable photographic images.
18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification.
   a. Examples:
      1. Weight
      2. Unique Tattoo
Methods to De-Identify:

- Use a code or another means to identify records . . . but make sure that code (or other method) is not:
  - derived from or related to the information about the individual; and
  - could not be translated to identify the individual.

- Example of what **not** to do:
  - Reverse the order of patient’s initials, weight, admission date(s), etc.
Minimum Necessary

- When using or disclosing PHI, or when requesting PHI from others, you must make reasonable efforts to limit the information to "the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."

- The minimum necessary standard does not apply to PHI uses and disclosures:
  - by/among health care providers for treatment purposes; or
  - to the individual who is the subject of the information, or in response to an authorization requested by that individual.
What does the “Minimum Necessary” rule mean to you as a student?

• Use or disclosure of PHI for educational purposes is considered a “health care operation”.

• So PHI may be used by and disclosed to health care students without the patient’s consent, agreement or authorization.

• HIPAA does place certain limitations on the use of PHI for educational purposes:
  1. The minimum necessary standard applies to uses and disclosures of PHI made for training and educational purposes. So whenever possible, specific PHI, such as the patient’s name, should not be used when discussing patients for educational purposes;
  2. The student who accesses PHI must protect and safeguard that information and properly dispose of any notes or class documents that contain PHI immediately on completion of the use or purpose;
  3. The student must be aware of and honor any agreed-upon restriction.
Allowable educational access to PHI:

You may use /access/share PHI for:

- Treatment
- Observation
- Teaching Rounds
- Retrospective Record/Data Reviews
- Case Presentations
- Patient Logs
Do’s and Don’ts: Treatment & Observation

Can Do:
- Access medical records of the patients you are treating/caring for
- Prepare class work with patient identifiers removed
- Observe patient care with approval from department manager/supervising faculty

Cannot Do:
- Obtain medical records of patients you are not treating/caring for!
- Use data obtained from your cases with patient identifiers such as name, address, birth date left in
- Observe patient care without appropriate approval or where the patient objects
## Do’s and Don’ts: Retrospective Reviews

**Can Do:**
- Access medical records with written approval of supervising faculty member
- Prepare class work using collected data with patient identifiers removed
- Use aggregate or de-identified patient information

**Cannot Do:**
- Use information collected for research without appropriate approval
- Publish or publicly present findings without appropriate approval or waiver of authorization
- Contact the patient or the patient’s physician
- Abstract patient identifiers
Scenario #1

Question:
As a student I am here to learn and today I heard about a very unusual case in the OR. I need to know more about the details so that I may gain a better understanding of the patient’s clinical course. I plan to review the records before I leave for the day. Is this okay?
Scenario #1 (cont.)

Answer: No.

While it might be argued that the student will obtain an educational benefit by reviewing unusual cases, such review must be formally requested and approved.

Individual access to patients’ records in this type of situation is not appropriate.

Electronic records and systems are monitored for inappropriate access.
Oral Discussions of PHI:

- Students and instructors should only discuss PHI as necessary to share required information and the treatment plan.
- Every effort should be made to protect the privacy of the patient by minimizing risk that others can overhear the conversation.
- The discussion of PHI should never occur in public areas such as the cafeteria or elevators.
- Discussions can occur at the nursing station and with a patient in a treatment area.
- Discussions may occur in a private classroom setting with your instructor.
Clinical Care Plans and Pre-Lab Reports

- **Care Plans and Pre-Lab Reports:**
  - **Cannot** contain any of the 18 PHI factors – they must be properly de-identified.
  - Used solely for education and treatment purposes.
  - Safely guarded and kept strictly confidential (between student/instructor).
    - If you leave your clinical site with a Care Plan and/or Pre-Lab Report, ensure that (i) it is properly de-identified, (ii) it is kept safe and not shared with anyone other than your instructor, and (iii) it is properly shredded or disposed of when it is no longer needed for educational purposes.
  - May be emailed if they have been de-identified and your instructor approves beforehand.
    - **Only use your methodistcollege.edu account to send and/or receive a Care Plan and/or any other information related to your clinical.**
  - **Remember:** You signed an agreement before starting your Clinical wherein you agreed to comply with HIPAA and ensure that a patient’s information be kept confidential and only disclosed when appropriate.
There are a variety of ways in which your use of social networking sites could result in a HIPAA violation:

- FaceBook,
- Foursquare,
- Twitter,
- Blogs,
- Instagram
- Etc.
Social networking can violate HIPAA!

- A nurse posted a patient’s picture and chart on his FaceBook page because he thought it was “funny;” since it was only “FaceBook,” there was no real harm in it.
- A doctor treated a patient over Twitter.
- ER personnel posted pictures on the Internet of a man being treated for fatal knife wounds.
- A doctor who asked a patient for a date after seeing her profile on dating website.
- A doctor was fired from a hospital in Rhode Island and reprimanded by the Board after she posted on her FaceBook page about a long day at work. She never referred to the patient’s name but gave enough details about the injuries to allow others to guess who it was.

**SUMMARY:** Even seemingly innocent behavior like writing about what you did at work on a blog or “friending” a patient on a social networking site can be a HIPAA violation!
How to avoid violating HIPAA on social media:

Except as necessary to share required information and patient treatment plans, **do not** talk about patients, even in general terms.

- **Example** of *inappropriate* post to Internet: “We had a fifty-year-old male in the ER last night with alcohol-induced liver disease.”
  - (Somebody looking at that post may respond to the post by saying: “Really? In Omaha? Hey – where were you last night? He’s fifty. Oh – I feel terrible for the kids.”)

- What if you just said: “Had a patient in the ER last night with alcohol-induced liver disease”?
  - It only takes a couple of clues about the poster, what he does, where he is, etc. to piece something together. As little as time frame or geography, coupled with conditions, can be enough.
Tips (cont.):

- If you wouldn’t say it on an elevator, don’t put it on-line!
- Check the tone of your social media presence.
  - If you are using social media to vent about your clinical experience, you should pause and evaluate – too much could be an early warning sign of trouble.
5 mistaken beliefs re HIPAA violations:

1. **It’s Private**
   - When posting anything clinical or practicum related on any social media site, you need to remember that it could end up anywhere. **On social media, even private posts are not private!**

2. **I can delete my post**
   - Enormous server farms are constantly scouring the web, preserving every scrap of date. Even if you post something and delete it just a few moments later, it’s still alive in the digital world and could come back to haunt you.

3. **It’s okay if I don’t use a name**
   - PHI is only safe to use when stripped of all 18 identifiers. Particularly in small communities, any innocent comment about a patient may help others identify the subject of the post.
5 mistaken beliefs re HIPAA violations: (cont.)

4. **She/He started it**
   - My patient posted her PHI on her own site, so I am free to comment, like, share or re-tweet it. A patient can disclose his or her own PHI, but if you share or re-tweet it on your personal accounts, you are giving it new life, and this land you in hot water.

5. **Name Omission**
   - Omitting a patient’s name, and other PHI, does not guarantee that the person cannot be identified. The uniqueness of a situation alone could allow people to reasonably identify a patient.
Safeguarding Information

**Must Do:**
- Password protect laptops, Smartphones, tablets, and any other mobile devices. **Know where they are at all times!**
- Be cognizant at all times of where your care plans are located and that they **do not** contain PHI.
- Shred facially de-identified papers when you are done with them.
- Insure memory/hard drive has been wiped clean when selling/disposing of a PC, laptop, Smartphone, tablet or mobile device.

**Cannot Do:**
- Leave information in open or other public areas.
- Discuss patients in elevator, hallways, or the cafeteria.
- Dispose of facially de-identified information in your trash can (it is still identifiable under HIPAA!).
- Share your access codes/cards.
To protect PHI and other confidential information, always keep your password confidential and follow these simple rules:

- Your password should be at least 8 characters in length.
- Your password should include 3 out of the following 4 categories:
  - An UPPER CASE alpha character.
  - A lower case alpha character.
  - A number
  - A symbol (* ! #)
- Change your password every sixty (60) days.
- Do not share your password with anyone!
Security of Mobile Devices

- Because of the risk of loss or theft of mobile devices . . .
- PHI should never be stored on or transferred to mobile devices unless you have received specific approval from your supervisor and the IT department to ensure security of information on the mobile device.
- Mobile devices include laptops, tablets, smart phones, flash drives, etc.
Photos and Videos

- DO NOT take photographs or videos at any time in your clinical or practicum using any mobile device or camera.
- NEVER post pictures or video of patients on social media websites or elsewhere on the internet.
E-mail

• Limit the information you include in e-mails to the minimum necessary for your clinical experience.
• If you must e-mail a Care Plan or any other patient related information to an instructor or fellow student, make sure it does not contain any PHI.
• Only use your methodistcollege.edu account to send and/or receive a Care Plan and/or any other information related to your clinical.
Penalties for HIPAA violations:

- HIPAA includes both **criminal** and **civil penalties** for:
  - Failure to comply with HIPAA requirements
  - Knowingly or wrongfully disclosing or receiving individually identifiable health information
  - Obtaining information under false pretences
  - Obtaining information with intent to:
    - Sell or transfer it
    - Use it for commercial advantage
    - Use it for personal gain
    - Use it for malicious harm
NMC penalties for HIPAA violation:

- In addition to civil and/or criminal penalties, you may also be:
  - *Expelled* from participation in the clinical experience at your designated site and any future clinical sites;
  - Ineligible for licensing; and
  - Subject to *disciplinary action* by NMC.
Reporting HIPAA Issues

- **How to report a HIPAA issue or concern:**
  - Reports may be made anonymously by calling the MHS Compliance Reporting Hotline at 877-640-0005 (English) or 800-216-1288 (Spanish), or electronically by using the [MHS Compliance Reporting link](#).
  - Talk to your instructor or supervisor.
  - Contact the NMC Chief Compliance Officer, Lindsay Snipes, at (402) 354-7259.
Question:
My friend was admitted to the hospital yesterday after collapsing during a bike ride. I am very concerned about her progress and would like to visit her but I don’t know which room she is in. Is it okay if I look up her information in the hospital computer system?
Scenario #2 (cont.)

Answer: No.

Using your access privileges to look up any information for any patient when there is no work or education related need to know is a violation of HIPAA. You will be subject to discipline for such a violation.
Scenario #3

Question:
The spouse of a patient I am seeing approached me in the hallway and asked me questions about the patient.
During my assessment visit, the patient indicated that she did not want information shared with her spouse.
What should I do?
Scenario #3 (cont.):

**Answer:**
Competent adult patients have a right to choose who is involved in their care and treatment. They can decide they do not want family members or others involved in their care. You should not share any information with the spouse if the patient has so requested and you should alert the nursing staff about the patient’s request.
Acknowledgements

- Green and Associates, Los Angeles, CA
- KevinMd.com
- U.S. Department of Health and Human Services
- University of Hawaii
- The University of Chicago
Acknowledgement Form

- By signing this form, I attest to having received and reviewed the HIPAA Training, which outlines the definitions and examples of HIPAA, policies, and responsibilities and expectations of employees, students, and staff at Nebraska Methodist College.

- I have also familiarized myself with the contents of this training. By my signature below, I acknowledge, understand, accept and agree to comply with the information contained herein.

- ______________________________________
  (Signature)

- ______________________________________
  (Date)

*Return this page either electronically or by hand to your instructor or compliance officer.*