WVU Health Sciences Center

Applying HIPAA and HITECH

HSC Privacy Office

So, what is HIPAA/HITECH?

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Privacy Rule
  - Security Rule
- Health Information Technology for Economic and Clinical Health Act (HITECH)
  - Adds “teeth” to HIPAA, enforcement, audits, state AG actions

So, what is HIPAA/HITECH?

- HIPAA Privacy Rule
  - Concerned with maintaining the privacy of patient information (electronic or paper).
- HIPAA Security Rule
  - Concerned with maintaining safeguards protecting electronic PHI.

Why Do HIPAA/HITECH Matter?

- Law
  - Civil, criminal penalties for individuals, institution
- Policy
  - HSC, WVUH, UHA Policies
  - HSC & WVU IT Policies
- Accountability/Transparency/Integrity
  - To patients
  - To the institution
  - To students, residents, faculty, and staff

What's at stake?

- Civil Penalties (Money Damages)
  - Range from $100.00 to $1.5 Million!
- Criminal Penalties (Possible Jailtime)
  - Fines from $50,000.00 to $250,000.00 and
  - Imprisonment for up to 10 years
  - Criminal charges can be brought against employees of covered entities
- @ WVU
  - Investigation of possible violations by HIPAA Investigative Team
  - **Discipline up to and including loss of employment, expulsion from program**

The Details

What You Need to Know About HIPAA as a health care provider

The Devil is in the Details

What is “PHI”?

- PHI is
  - Information created or received by a health care provider (that’s you!), health plan, or health clearinghouse
  - **Relating to past, present, or future health of an individual, provision of health care, or payment for health care**
  - **Either identifies the individual or provides a “reasonable basis” for identification**
  - Information in all forms (oral, written, or electronic)

Details – Privacy Rule

- HIPAA Privacy Rule
  - A covered entity may not use or disclose protected health information, unless an exception applies
  - There are **only three reasons** a faculty member, resident, or student could legitimately have PHI outside of the medical record
    - Valid, HIPAA-compliant authorization from the patient for a legitimate purpose
    - IRB protocol in place and being followed as it pertains to PHI
    - It is not really PHI, meaning it is de-identified information about a patient
  - If you have it for any other reason, think you need it for any other reason, or know anyone else has it for any other reason, you should seek guidance about what to do **before you do it**

Where SHOULD I be keeping PHI?

- #1 – If it relates to treatment, payment or health care operations in **any way** it should **always** be in the medical record and **only** be in the medical record, unless:
- #2 – You have a legitimate reason to keep it i.e. teaching, research, or Boards, and it should either be de-identified, you should have a specific authorization on file, or an IRB protocol in place.

The Golden Rules

- Use information only when *necessary* to perform your responsibilities.

- Use only the *minimum* amount of information necessary to perform your responsibilities.

Verbal

- Be aware of your surroundings at all times when discussing patient information.
  - Do not discuss patient information in public spaces such as open hallways, elevators, or the cafeteria.

- Before discussing a patient's condition, treatment, or other protected health information (PHI) with his/her family member(s), determine if the patient would object to such a disclosure, and be as discreet as possible if in an area where other patients / families are sitting.

Verbal

- Do not leave telephone messages that include PHI.
- Know to whom you are speaking (visitor, patient, family member).
  - If information is requested via telephone, confirm the patient's birth date and confirm the disclosure is appropriate.
- Do not discuss ANY PHI with other residents (that are not on your team), family, or friends unless authorized to do so or an exception applies.

Written

- Dispose of patient information in designated confidential shredding bins at the conclusion of each day or at the conclusion the patient's treatment.
  - Do NOT dispose of in regular trash bin.
- Check printers, faxes, copy machines when you are finished using them.
- Return any paper charts or patient files to their designated areas, and ensure they are secured.

Electronic

- **Do NOT search for yourself or any family members, friends, or other employees in the electronic medical record (EMR).**
- **UTILIZE MyWVUChart to view your own information and get proxy access for your spouse and kids 12-18 yo.**
  - Do not view the EMR of patients who are not on/related to your service.
- If a colleague asks you to look at something in their chart because it's your specialty . . . DOCUMENT IT!
- Do not allow others to access the EMR under you credentials, and do not access the EMR under credentials other than your own.

Electronic

- Ensure your computer, laptop, and iPad/tablet are physically secured in locked areas when left unattended.
- Create a strong password and do NOT share your username/password with anyone.
  - Password/Pin protect mobile devices and tablets
- Do not keep PHI or confidential data on portable devices without proper authorization from Information Security.
- Ensure your devices have necessary anti-virus, security updates, and encryption software installed.

Electronic

- Social Media Policy: It's an acceptable form of communication if, and only if, the communication is professional and complies with federal and state law.
  - Keep your professional activity separate from your personal social media activity.
  - Never post patient information on Social Media!

Privacy Breach

- Physically lost or stolen information
  - Paper copies of patient information
  - Electronic devices containing PHI

- Misdirected information
  - Verbal messages left for the wrong person
  - Mislabeled mail
  - PHI placed on social media

Reporting a Privacy Breach

- Report breaches/potential breaches in a timely manner.
  - Not reporting will result in more severe disciplinary action.

- Report a concern or potential breach of Protected Health Information by contacting the WVU HSC Privacy Office at (304)293-3584 or WVUH Privacy Office at (304)598-4109.

- If you lose something with PHI on it (electronic or written), notify your supervisor and the Privacy Office immediately!

Summary

- It can be easy to dismiss HIPAA as just another law or a required training we have to do at the beginning of every year

- It’s very likely you will see violations of HIPAA occur every day while you are on rotations, BUT remember :
  - It never makes it okay or acceptable
  - You are responsible for your actions
  - Don’t be afraid to remind your colleagues of their duties regarding patient privacy (we’re a team!)

- Please remember there can be serious consequences for a HIPAA privacy breach.

QUESTIONS?

WVU – HSC Privacy Office

(304) 293-3584

WVU – HSC IT Security Office

(304) 293-4683

For useful privacy tips and tools, follow us on Twitter:

@WVUHSCPrivacy