Protecting Patient Information
HIPAA Faux Pas

J. Brian Williams, D.O. FACOEP

Regional Medical Director, TEAMHealth

TEAMHealth

What is HIPPA?

Health Insurance Portability and Accountability Act

- Signed into law Aug 21, 1996
- Contains 5 sections or titles
- Title II is directs US Dept of HHS to develop national standards for processing electronic healthcare transactions

TEAMHealth

What does HIPAA do?

- Establishes standards to protect an individual's personal health information
- Sets limits and conditions on the use and disclosure of such information without the individual's authorization
- Allows the individual to have oversight of their personal health information

TEAMHealth

What is Protected Health Information (PHI)?

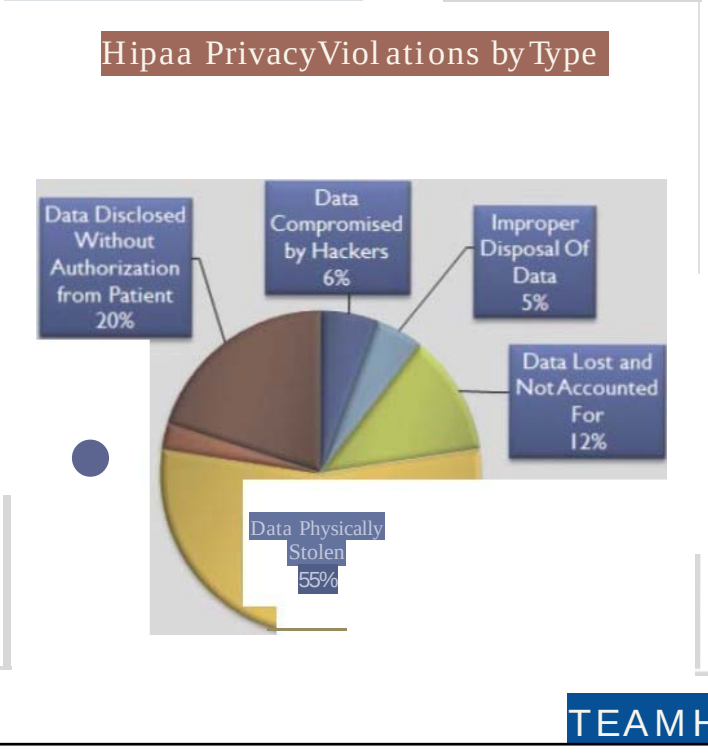
- Individually identifiable health information in any form or medium
- Relates to past, present, or future physical or mental health condition of an individual
- Includes the patient's demographic information, medical record, and payment history

TEAMHealth

Minimum Necessary Requirement

- An entity covered by HIPAA must make reasonable efforts to use, disclose or access the minimum amount of PHI needed to accomplish the intended purpose
- Always ask before you access, "Is this PHI necessary to perform my job?"
- Note that the Minimum Necessary rule does not apply when disclosing information (1) to the patient who is subject of the information or (2) to another healthcare provider for treatment purposes

TEAMHealth



TEAM Health

Top Five HIPAA Settlements of 2016

- $5.5 Million- Advocate Health Care (Downers Grove, Ill.) - 3 incidents compromised the ePHI of 4M individuals
  - 4 laptops stolen from an office
  - External party accessed a Business Associates' Network
  - Laptop stolen from employee's vehicle
- $3.9 Million- Feinstein Institute for Medical Research (Manhasset, N.Y.)
  - Laptop stolen from employee's car-ePHI of 13,000 patients and research participants was compromised
- $2.75 Million- University of Mississippi Medical Center (Jackson)
  - Laptop stolen by hospital visitor-ePHI of approximately 10,000 patients was compromised
- $2.2 Million- Oregon Health & Science University (Portland)
  - Laptop stolen from surgeon's vacation home
  - Physician residents were storing ePHI in a Google based cloud system without contractual relationship
- $2.14 Million- New York-Presbyterian Hospital (New York City)
  - TV crews filmed patients for the ABC show "NY Med" without the patients' permission

TEAMHealth

HIPAA DOLLARS

- From April 2003 to February 28, 2017, the OCR has collected over $67M dollars in fines, penalties and settlements.
- Over $39M of that $67M has been collected since January 1, 2016 ……. 14 months!

TEAMHealth

HIPAA Faux Pas #1: Unauthorized Access

- *Activity:* Because you're granted log-in credentials, you access the EMR of a high profile patient, celebrity, family member, ex-spouse, child, or other
- *Outcome:* Unauthorized or inappropriate access could result in a privacy breach
- *Lesson Learned:* You must only access PHI of patients that you have a treatment relationship. Access to your own personal or family member records should be done in accordance with hospital policy

TEAMHealth

HIPAA Faux Pas #2: Discharge Paperwork

- *Activity:* In a busy ED, you grab paperwork from the only printer and provide it to the patient while reviewing the discharge plan. Patient arrives home to find the paperwork is for another patient
- *Outcome:* This resulted in inappropriate disclosure of PHI and possibly a privacy breach
- *Lesson learned:* Always confirm the paperwork is for the correct patient before it is presented to the patient

TEAMHealth

HIPAA Faux Pas #3: Posting to Social Media

- *Activity:* Abdominal x-ray of foreign object is posted to Facebook with comment "This is a first in our ED." You have removed patient name or other unique identifier prior to posting on FB (doesn't matter)
- *Outcome:* Several ED staff are FB friends and report it to administration; hospital Peer Review/Med Exec review case; inappropriate disclosure of PHI and possibly privacy breach
- *Lesson learned:* PHI should never be posted to social media, even if you attempt to remove patient identifiers

TEAMHealth

HIPAA Faux Pas #4: Family & Friends Present

- *Activity:* You discuss the patient's lab and CT results with the patient while family and friends are in the room
- *Outcome:* Patient complains to hospital that he did not want the results known to those present in the room; this may result in a possible privacy violation
- *Lesson learned:* Tell the patient you would like to discuss his/her health information and ask if friends/family should leave the room or provide the patient the opportunity to object

TEAMHealth

HIPAA Faux Pas #5: Personal Mobile Device Photos

- *Activity:* Cardiologist requests copy of EKG prior to coming to ED and you text photo of EKG taken with your cell phone
- *Outcome:* Privacy violation not likely if the EKG is sent to the correct recipient; however, photos containing PHI are now located on cardiologist's and your cell phone (what about loss/theft of device; further disclosure to unauthorized person)
- *Lesson Learned:* We encourage you to follow hospital policy for texting PHI and utilizing an encrypted means of transmission; PHI should never be stored on personal mobile devices

TEAMHealth

When a Privacy Breach Occurs

- Reputational harm; loss of patient trust
- Notification to patient and Office for Civil Rights
- Civil Sanctions: $100 - $50,000 per violation with max penalty of $1.5M/year
- Criminal Sanctions: If knowingly or with false pretenses to obtain or disclose PHI, fine up to $100,000 & imprisonment up to 5 years

TEAMHealth

Take Aways

- Only access the minimum necessary to perform your job
- Never post PHI to social medical or share with unauthorized individuals
- Be aware of your surroundings and only discuss PHI that you are authorized to share
- Confirm any correspondence to or communication with the patient is directed to the correct individual
- Report all inappropriate use, disclosure, or access of PHI to your supervisor or to TeamHealth Compliance